RouteFinder™

Multi-Protocol Router with T1 DSU

Multi-Protocol Router with Internal T1 DSU

Model MTASR2-203

User Guide

MultiTech® Systems

User Guide

S0000007 Revision A

RouteFinder (Model MTASR2-203)

Record of Revisions

Revision	Description
A (7/15/99)	Manual released. All pages at revision A.

Patents

This Product is covered by one or more of the following U.S. Patent Numbers: **5.301.274; 5.309.562**; **5.355.365; 5.355.653; 5.452.289; 5.453.986**. Other Patents Pending.

TRADEMARK

Trademark of Multi-Tech Systems, Inc. is the Multi-Tech logo. RouteFinder is a trademark of Multi-Tech Systems, Inc.

Windows is a registered trademark of Microsoft Corporation in the United States and other countries.

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(612) 785-3500 or (800) 328-9717
Fax 612-785-9874
Tech Support (800) 972-2439
BBS (612) 785-3702 or (800) 392-2432
Internet Address: http://www.multitech.com

Contents

Chapter 6 - Service, Warranty and Tech Support

Appendixes

Glossary of Terms

Index

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 1 - Introduction and Description

MultiTech® Systems

Introduction

Welcome to Multi-Tech's new RouteFinder™, model MTASR2-203, providing secure and seamless LAN-to-LAN routing capability over a Point-to-Point T1 or Fractional T1 (FT1) service.

The MTASR2-203 supports several LAN-to-LAN configurations and a wide range of routing protocols including IP and IPX routing with MAC-layer bridging for all other protocols.

- The most common configuration is the internal T1 DSU connected through a T1 facility to a site with a modem or ISDN TA backup connected to the RS-232 port (maintains connectivity in case the T1 facility goes down).
- A second configuration may be the same internal T1 DSU connected to a T1 facility using frame relay (When frame relay is being used, only the internal T1 DSU is used).
- A third configuration is an internal T1 DSU connected to the same T1 facility with a second T1 facility connected to the RS-232/V.35 port to a second site (No back-up resource can be provided with this two-LAN configuration).

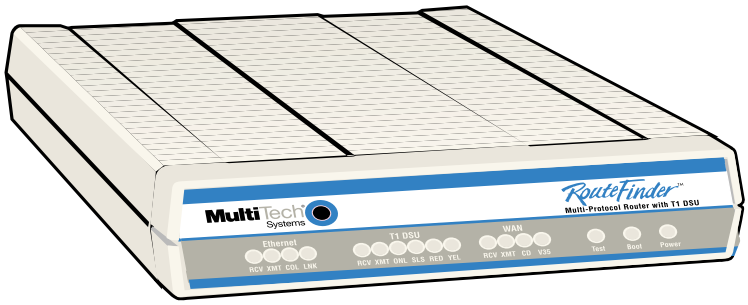


Figure 1-1. RouteFinder

The RouteFinder features a 10Base-T for your LAN connection, a Command port for configuration, an internal T1 DSU for T1 connectivity, and an optional RS-232/V.35 port for a second T1 connection or dial back-up connectivity. The RouteFinder supports data rates up to 1.536 Mbps, D4 or Extended Super Frame (ESF) framing format, and AMI or B8ZS line coding.

System management is provided through the Command port using bundled Windows software that provides easy-to-use menus.

Preview of this Guide

This guide describes the RouteFinder and explains how to install and configure the unit. The information contained in each chapter is as follows:

Chapter 1 - Introduction and Description

Chapter 1 describes the RouteFinder, including the front panel indicators, back panel connectors, shunts, and lists the relevant specifications.

Chapter 2 - Installation

This chapter provides information on unpacking and cabling. The cabling procedure describes the cable connection to the Ethernet LAN, to a PC for configuration, to an internal T1 DSU, and AC power. If the optional WAN 2 port is to be used, then the cabling procedure describes the cable connection to an external WAN.

Chapter 3 - Software Loading and Configuration

Chapter 3 describes the RouteFinder-T1 software loading procedure and configuration of the RouteFinder for IP, IPX, or Spanning Tree Protocol. The physical WAN port is configured for synchronous or asynchronous communication. The RouteFinder software diskettes are Windows® - based.

Chapter 4 - RouteFinder Software

Chapter 4 describes the RouteFinder software package designed for the Windows® environment. The RouteFinder Program Group has seven icons that allow for configuration, download default setup, download firmware update, and local port setup.

Chapter 5 - Remote Configuration and Management

Chapter 5 provides procedures for changing the configuration of a remote RouteFinder. This chapter also describes typical Telnet client and Web-browser management of the RouteFinder.

Chapter 6 - Service, Warranty and Tech Support

Chapter 6 provides instructions on getting service for your RouteFinder at the factory, a statement of limited warranty, information about our Internet presence, and space for recording information about your RouteFinder prior to calling Multi-Tech's Technical Support.

Front Panel

The front panel contains four groups of LEDs that provide the status of the LAN connection, the T1 DSU activity, WAN Link activity, and general status of the RouteFinder. The Ethernet LEDs display the activity of the LAN whether the RouteFinder is connected to the LAN, transmitting or receiving packets, and if a collision is in progress. The T1 DSU LEDs show whether the T1 is on line or in a failure mode. The WAN Link LEDs display the status of the link (i.e., ready to transmit or receive serial data and if an external communications device with a V.35 interface is connected to the RouteFinder). The last group of LEDs indicates whether the self test passed or failed, if the unit is in the process of rebooting, or if the power On/Off switch on the back of the RouteFinder is turned On.

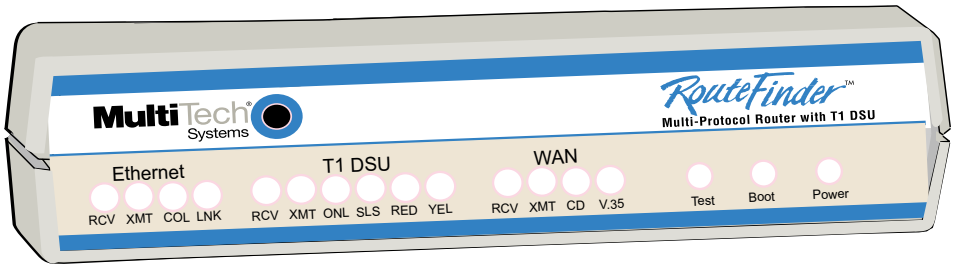


Figure 1-2. Front Panel

Ethernet

RCV Receive indicator blinks when packets are being received from the local area network.

XMT Transmit indicator blinks when packets are being transmitted to the local area network.

COL Collision indicator lights when a collision is in progress, that is, when two nodes are transmitting packets at the same time.

LNK Link indicator lights indicating that the RouteFinder is connected to the local area network.

T1 DSU

RCV Receive indicator blinks when packets are being received from the wide area network.

XMT Transmit indicator blinks when packets are being transmitted to the wide area network.

ONL Online lights whenever a carriage signal is detected and no error conditions are present.

SLS Sync Loss lights when there is a loss of sync in the signal output.

Red Warning lights when there is a red alarm on the T1 line.

Yel Warning lights when there is a yellow alarm on the T1 line.

WAN Link

RCV Receive indicator blinks when the link is receiving data.

XMT Transmit indicator blinks when the link is transmitting data.

CD Carrier Detect indicator lights when the RouteFinder detects a carrier signal.

V.35 The V.35 indicator lights when the link is configured for a V.35 interface. That is, the shunt for the link is in the V.35 position.

Test The Test indicator lights (green) while performing the T1 test.

Boot The Boot indicator lights (green) while the RouteFinder is in the process of coming up (normal mode).

Power The power indicator lights when the On/Off Switch is in the ON position.

Back Panel

The cable connections for the RouteFinder are made at the back panel. The cable connectors on the back panel are shown in Figure 1-3 and defined below.

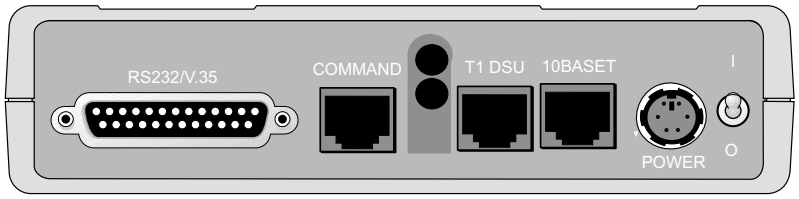


Figure 1-3. Back Panel

RS-232/V.35 Connector

The RS-232/V.35 connector is used to connect the RouteFinder to a WAN device (used primarily for Dial back-up). The WAN device connection is to an asynchronous or synchronous communications device such as a modem, DSU, or ISDN terminal adapter. This connection can be either RS-232C or V.35. If the connection is V.35, then the shunt must be moved from the default RS-232 position to the V.35 position. This connector is a DB25 male connector.

Command Port Connector

The Command Port connector is used to configure the RouteFinder using a PC with a serial port and running Windows® software. The Command Port connector is an RJ-45 jack and a short adapter cable is provided to convert to a standard serial port DB9 female connector.

Monitor Jacks

The Monitor jacks (for Bantham plugs) are used by Telco personnel to connect T1 test equipment. This would become necessary in case of bad lines or other transmission problems. The upper jack (Receive) monitors receive data on the T1 line; and, the lower jack (Transmit) monitors transmit data on the T1 line.

T1 DSU Connector

The RJ-48 T1 DSU jack is used to connect a point-to-point T1 line from your local Telco.

10Base-T Connector

The 10Base-T connector is used to connect the RouteFinder to a LAN using unshielded twisted cable. This connector is an RJ-45 jack.

Power Connector

The Power connector is used to connect the external power supply to the RouteFinder. The Power connector is a 6-pin circular DIN connector. A separate power cord is connected to the power supply and the live AC grounded outlet.

ON/OFF Switch

The power switch provides DC power to the RouterFinder when placed in the ON position and removes power when placed in the OFF position.

Shunts

A shunt on the RS-232/V.35 connector (WAN 2) port allows the same connector to be configured for an ITU-T V.35 electrical interface signaling or EIA-232C/D signaling. The ITU-T V.35 signaling levels are generally more reliable for high speed data and/or longer cable distances. The EIA-232C/D signaling is intended for data rates of 19.2 Kbps or less and cable lengths of 50 feet or less. For higher speeds and/or longer distances, the V.35 is generally preferred.

The shunt positions are toward the back of the printed circuit board (See Figure 1-4).

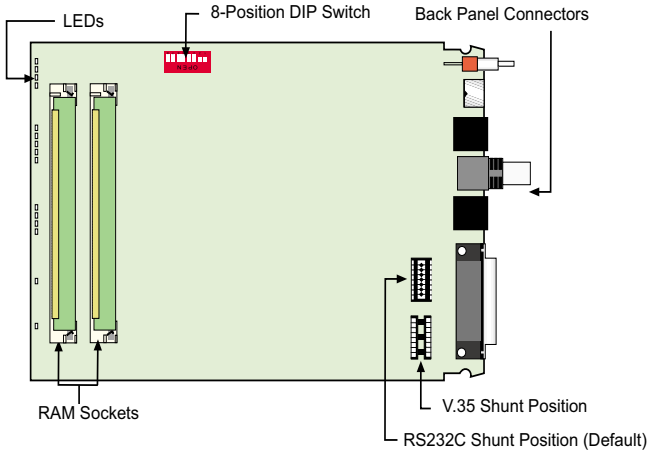


Figure 1-4. Shunt Positions

The RouteFinder has a shunt for the RS-232 and the V.35 links. The RS-232 and V.35 shunt positions are identified. To change the position of the shunt, refer to the V.35 “Changing Shunt Position” procedure.

Specifications

The RouteFinder conforms to the following specifications.

- Routing Protocols - IP and IPX and bridging for all others
- WAN Interface - 1 async or sync link (RS-232C/V.35)
- Command Port - 19.2 Kbps asynchronous
- T1 DSU - 1.544 Mbps synchronous
- Ethernet LAN Interface - 10Base-T (twisted pair)
- Two 4-megabyte DRAMs (1 meg by 36 bytes at 70 nanosecond SIMMs)

  Caution: SIMM speed and size cannot be mixed.
- 1 MB of Flash memory

WAN 2 Port

- 115.2 Kbps asynchronous RS-232/V.35 (WAN 2) or T1 (1.544 Mbps) sync link using DB25 male connector. Optional ITU-T V.35 interface using a V.35 adapter cable.

Command Port

- Single 19.2 Kbps asynchronous Command Port using a short RJ-45 to DB9 cable with a female connector.

T1 DSU Port

- Single T1 line port with synchronous data format
- AMI or B8ZS line coding
- D4 Super Frame or Extended Super Frame support
- 1 to 24 channels at 56 Kbps or 64 Kbps each
- RJ-48 jack

Ethernet Port

- One Ethernet Interface - 10Base-T (twisted pair) RJ-45 connector

Electrical/Physical

- Voltage - 115 VAC (Standard), 240 Volts AC (Optional)
- Frequency - 47 to 63 Hz
- Power Consumption - 10 Watts
- Dimensions - 1.625" high x 6" wide x 9" deep

  4.13 cm high x 15.24 cm wide x 22.86 cm deep
- Weight - 2 pounds (.92 kg)
- Temperature

  Operating: 32^{o} to 122^{o} F (0^{o} to 50^{o} C)
  Storage: 4^{o} to 158^{o} F (-20^{o} to 70^{o} C)
- Relative Humidity - Up to 95%, non-condensing

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 2 - Installation

MultiTech® Systems

Introduction

This chapter includes safety warning information and guides you through the unpacking and installation of your RouteFinder. The installation procedure, provides step-by-step instructions on cabling and powering-on your unit. Chapter 3 provides instructions on loading and configuring the software.

Unpacking

The shipping box contains the RouteFinder, external power supply, command port adapter cable (short cable with RJ-45 on one end and DB9 on the other), one RJ-48 cable for T1 DSU connection, your Quick Start Guide, and one CD-ROM with RouteFinder-T1 Install Software and MTASR2-203 User Guide. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the unit; contact Multi-Tech's Technical Support for advice (refer to Chapter 6). If no damage is observed, place the RouteFinder in its final location and perform the Cabling Procedure.

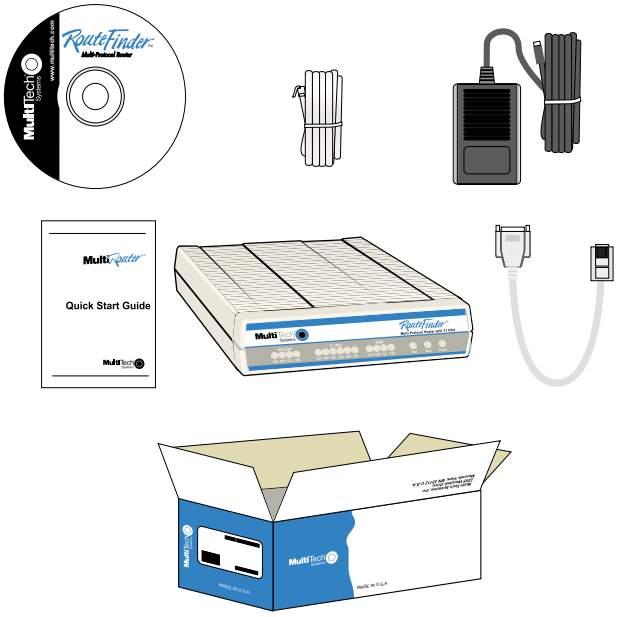


Figure 2-1. Unpacking

Safety Warnings

1. Never install telephone wiring during a lightning storm.
2. Never install a telephone jack in wet locations unless the jack is specifically designed for wet locations.
3. This product is to be used with UL and cUL listed PCs.
4. Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
5. Use caution when installing or modifying telephone lines.
6. Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electrical shock from lightning.
7. Do not use a telephone in the vicinity of a gas leak.
8. To reduce the risk of fire, use only 26 AWG or larger telecommunication line cord.

Cabling your RouteFinder

Cabling your RouteFinder involves connecting the Command Port, T1 DSU, Ethernet, and power . If the optional WAN 2 port (RS-232/V.35 connector) is used, refer to “Optional WAN 2 Cabling.” Figure 2-2 shows the back panel connectors and the associated cable connections. To connect the cables to your RouteFinder, do the following.

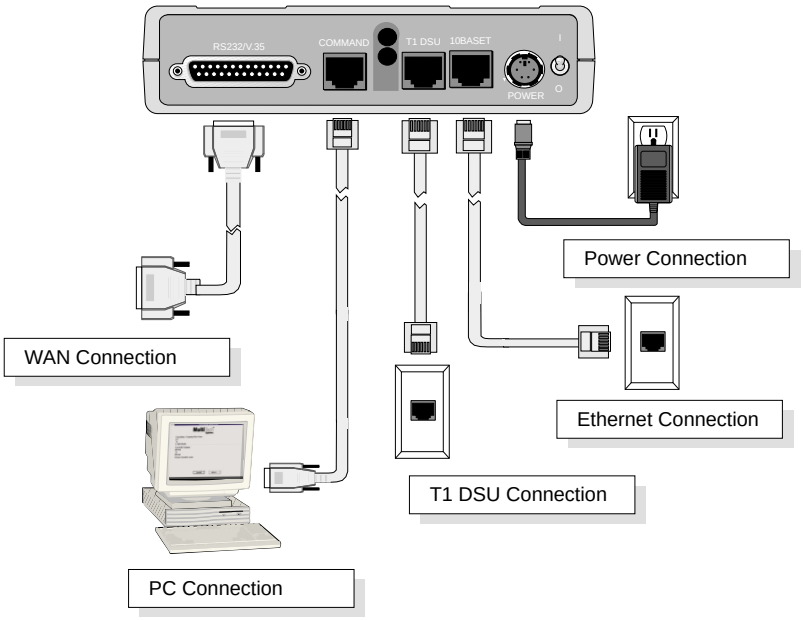


Figure 2-2. Back Panel Connections

1. Connect the RouteFinder to your PC using the short RJ-45 to DB9 (female) cable provided with your unit.

   Plug the RJ-45 end of the cable into the Command Port on the RouteFinder. Plug the other end (DB9 female connector) into a COM port on the PC. See Figure 2-2.

2. Connect an RJ-48 cable to the T1 DSU connector on the back panel connector and connect the other end to the T1 service.

3. Connect an Ethernet cable with an RJ-45 cable to the 10Base-T connector on the back panel connector and connect the other end to your Ethernet connector.

4. Connect one end of the power supply to a live AC outlet, then connect the other end to the POWER connector on the RouteFinder as shown in Figure 2-2. The power connector is a 6-pin circular DIN connection.

5. Turn on power to the RouteFinder by setting the ON/OFF switch on the back panel to the ON position. At this time your RouteFinder is completely cabled and powered On.

Optional WAN 2 Cabling

The MTASR2-203 provides an optional RS-232/V.35 port for a second T1 connection or dial back-up connectivity.

Note: If the WAN link needs to be changed to a V.35 interface, perform the “Changing Shunt Position” described in Appendix C.

1. Connect an RS-232C/D or V.35 interface cable to the back panel RS-232/V.35 connector as shown in Figure 2-2.

2. Connect the other end of the cable to the appropriate connector on the external link device (WAN connection).

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 3 - Software Loading and Configuration

MultiTech® Systems

Introduction

Before you start loading your software, you will need to contact your local telco to find out how your T1 service is being provided. The software loading procedure does not provide every screen or option in the process of installing the RouteFinder software. It is assumed that a technical person with a thorough knowledge of Windows and the software loading process is doing the installation.

Before You Start Loading Your Software

Contact your local telephone company that is providing your T1 service and ask for the folllowing: line coding (AMI or B8ZS), frame format (D4 or ESF), and available bandwidth (full T1 is 24 DSOs) or number of DSOs and which DSO assignments, if FT1. Record your provisioning information below:

Line Code: AMI/B8ZS _____

Framing Format: D4/ESF _____

Available bandwidth: Full T1 (24 DSOs), or _____

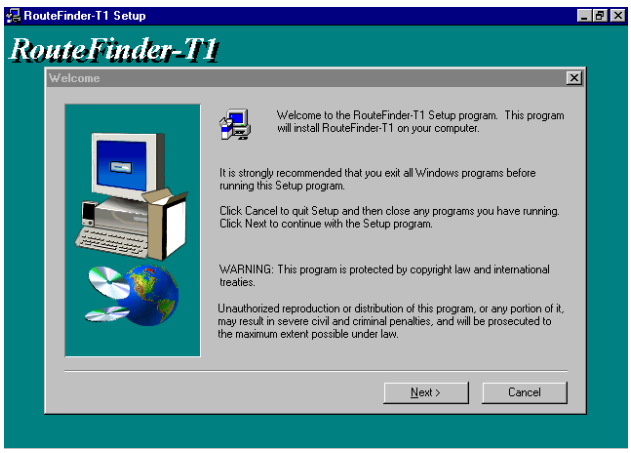
Number of DSOs and which DSO assignments, if T1. _____

Installing your Software

1. Insert the RouteFinder CD-ROM into a CD-ROM drive on your local PC. The CD-ROM starts automatically (It may take 10 to 20 seconds for the Multi-Tech Installation CD screen to appear).

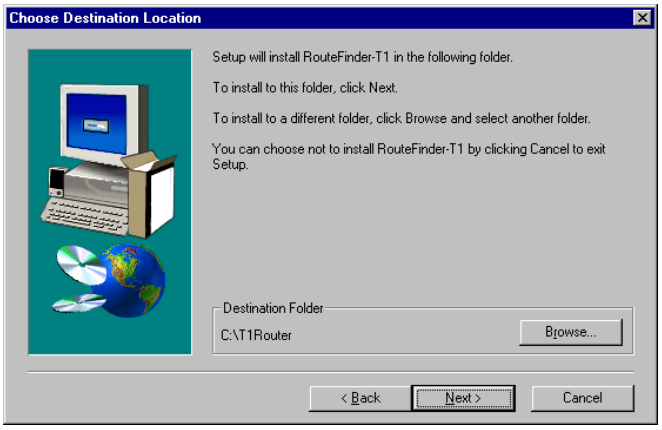
   If the Multi-Tech Installation CD Screen does not appear automatically, click **My Computer**, then right-click the CD-ROM drive icon and click **Autorun**.

2. When the Multi-Tech Installation CD Screen appears, click the **Install Software** icon.
3. Windows prepares the Install Shield and then displays the **Welcome Screen** dialog box.



   Press **Enter** or click **Next >** to continue.

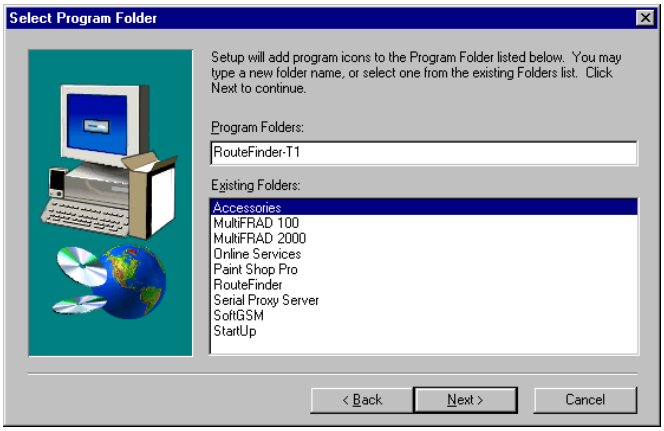
4. The **Choose Destination Location** dialog box is displayed.



If you accept the default Destination Folder, press **Enter** or click **Next >** to continue.

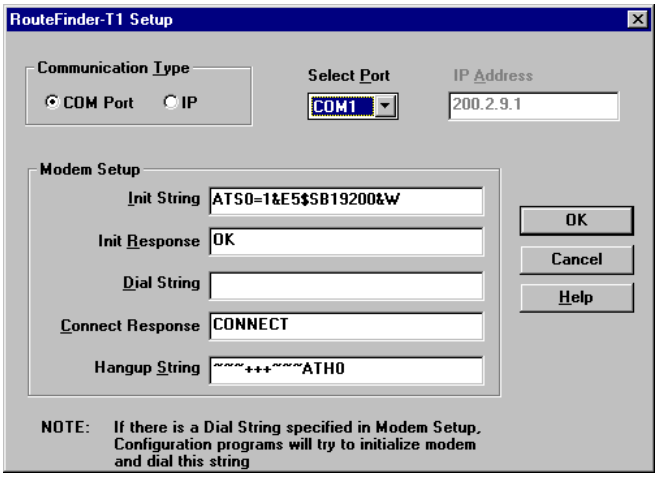
If you do not accept the default Destination Folder, click **Browse**, define your Destination Folder, and then press **Enter** or click **Next >** to continue.

5. The **Select Program Folder** dialog box is displayed. The word “RouteFinder-T1” in the Program Folders text box will become the name of the icon group.



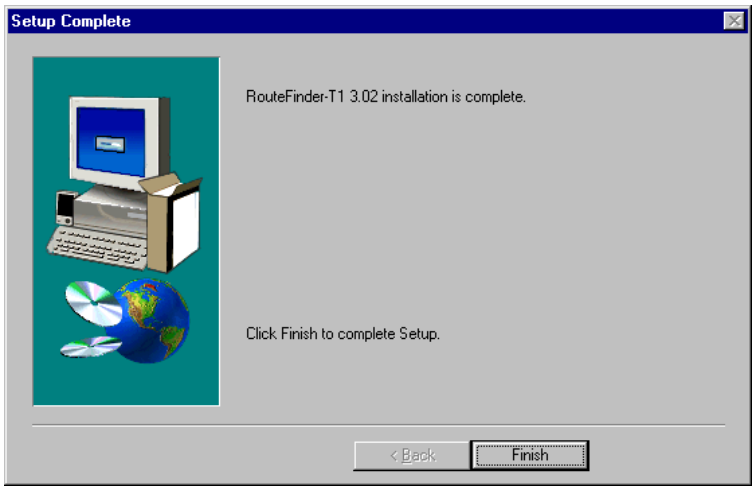
Press **Enter** or click **Next>** to continue.

6. The **Setup** dialog box is displayed allowing you to select the COM port of the PC that is connected to the Command Port of the RouteFinder. Next to the **Select Port** window, click the down arrow and choose the COM port of your PC (COM1 -- COM4) that is connected to the RouteFinder.



Click **OK** to continue.

7. The **Setup Complete** dialog box is displayed.



Click **Finish** to continue.

8. The **Setup** dialog box asking “Do you want to download default setup?” is displayed.

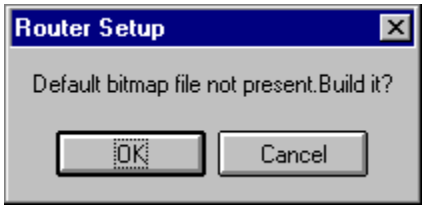
Click **Yes** to download the default setup.

Clicking **No** prevents the defaults from being downloaded to the RouteFinder. You are returned to the program manager, and in Windows 98/95/NT you will see an open window with shortcut icons for all the various utility programs provided in the RouteFinder software.

9. The **Default Setup** dialog box asking “Router is Running. Reboot to download setup?” is displayed.

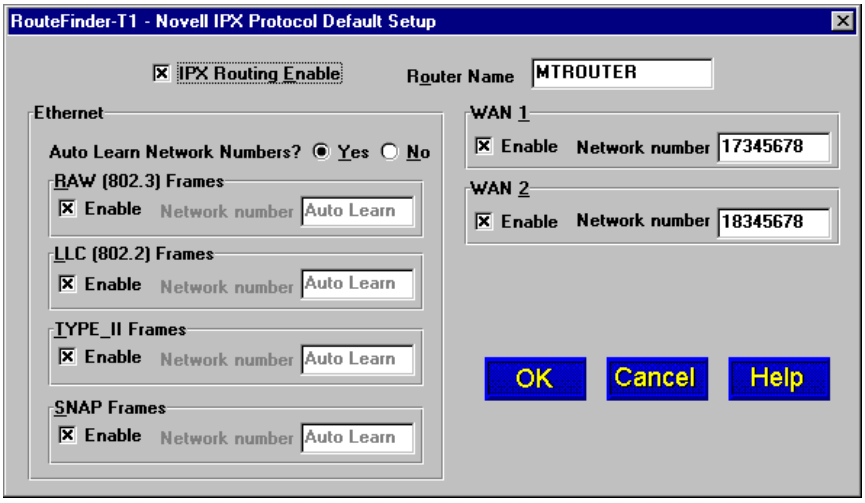
Click **Yes**.

10. The **Router Setup** dialog box is displayed.



Click **OK** to build the bitmap.

11. The **Novell IPX Protocol Default Setup** dialog box is displayed.



12. If your network protocol is **IPX,** continue with the following steps. However, if your network protocol is **IP**, click the **IPX Routing Enable** check box to *disable* IPX, then click **OK** and proceed to step 17.
13. **Router Name:** If this is the only RouteFinder on your network, you can use the default Router Name (MTROUTER); otherwise, you must assign a new Router Name in this field. The Router Name can be any printable ASCII string of up to 47 characters. The RouteFinder will use this name to advertise its service in the IPX internetwork.
14. **Ethernet:** You can enable **Auto Learn Ethernet Network Numbers** by leaving the default (**Yes**) checked, or you can manually assign the network numbers after disabling the Auto Learn option by clicking **No**. If no file server is connected to the Ethernet segment, then you should select **No**.

    If you enable Auto Learn, the RouteFinder will learn the IPX network numbers from the file server.

    If you disable Auto Learn, record in the space below the network numbers assigned by the network file server for each of the four frame types [(Raw (802.3), LLC (802.2), EthernetII (Type II), and SNAP]. Also record the Network number for WAN 1.

    RAW (802.3) Frames Network Number _____

    LLC (802.2) Frames Network Number _____

    TYPE_II Frames Network Number _____

    SNAP Frames Network Number _____

    WAN 1 Network Number _____

    WAN 2 Network Number _____

    When you manually assign network numbers, make sure they match the network numbers assigned to your local file server (if any).
15. **WAN 1**: enter the WAN Network number for the WAN port by clicking the Network Number box and back-spacing through the default numbers entering your new WAN number. The WAN network number must be the same as at the RouteFinder -T1 on the other end of the T1 service.

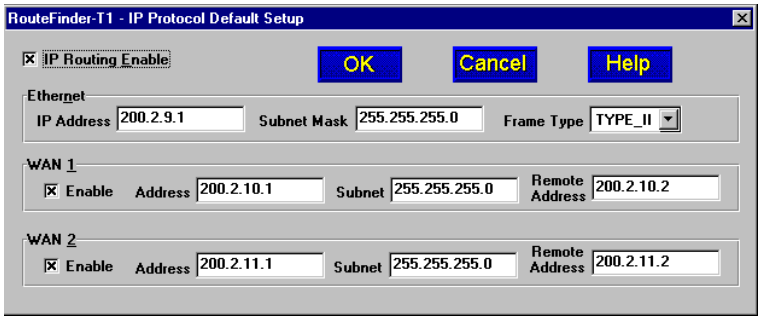
    The WAN network number has to be assigned by the network administrator and must be unique throughout the entire internetwork.

    WAN 2: if WAN 2 is to be used (e.g., for Remote Access or an additional network), enter the WAN network number for the WAN port by clicking the Network Number box, back-spacing through the default numbers entering your new WAN number. The WAN network number must be the same as at the RouteFinder on the other end.

    The WAN network number has to be assigned by the network administrator and must be unique throughout the entire internetwork.

    Note: The WAN ports do not have the capability of learning the network number (i.e., the WAN port does not have a file server).
16. Click **OK** when you are satisfied with your selections.

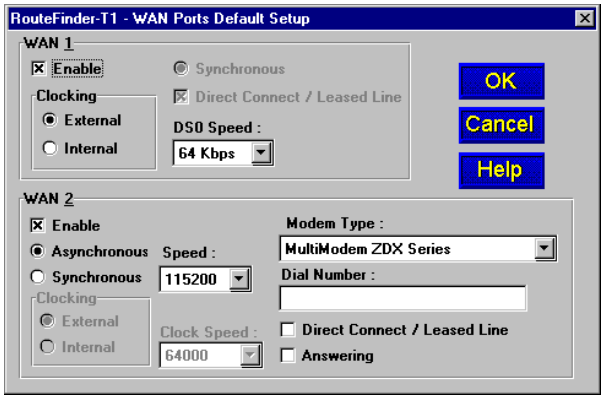
17. If you disabled IPX and then clicked **OK** from the IPX Protocol Default Setup dialog box (step 12), the **IP Protocol Default Setup** dialog box is now displayed.



18. To change the IP parameters, proceed to the next step. Otherwise, click on the **OK** button to open the **WAN Ports Default Setup** dialog box, then advance to step 24.
19. The default Ethernet IP Address has to be changed to your unique LAN address. Assign an acceptable unique **IP Address** to the Ethernet port.
20. Change the default **Subnet Mask** and **Frame Type** to the value assigned to your LAN port.
21. The default WAN 1 address has to be changed to your unique WAN 1 address. Assign an acceptable unique WAN 1 port address in the **Address** field.

    Change the default **Subnet** and **Remote Address** for the WAN port address to the values assigned to your WAN (applies to both WAN 1 and WAN 2).

    If WAN 2 is to be used (e.g., for Dial Back-up), the default WAN 2 address has to be changed to your unique WAN 2 port address in the WAN 2 **Address** field.
22. Click **OK** when you are satisfied with your selections.
23. The **WAN Ports Default Setup** dialog box is displayed allowing you to configure WAN 1 for a T1 connection and WAN 2 for an optional connection.



WAN 1: The **Clocking** option will most likely be **External**. If your T1 service requires Internal clocking, click the **Internal** option.

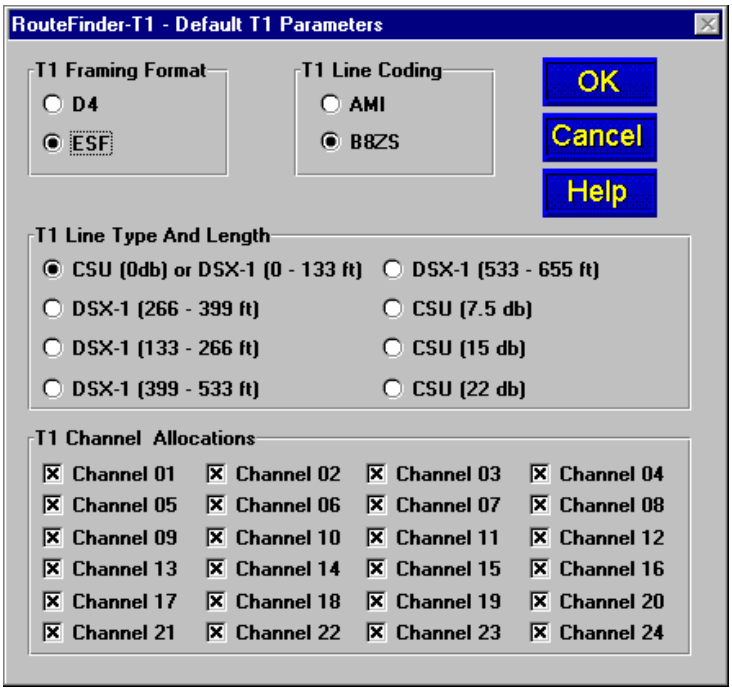
WAN 2: If the WAN 2 port is connected to a synchronous device, select **Synchronous**; the default uses an external clock in the synchronous device. If you are using the RouteFinder's internal clock, select **Internal Clock** and select the appropriate **Clock Speed** from the pull-down list.

If the WAN 2 port is connected to an asynchronous device, select **Asynchronous**. Note that the **Direct Connect / Leased Line** option must be disabled; if not, click (check) the box to disable it. The **Modem Type** and **Dial Number** fields become active. Select your external modem from the pull-down list. The **Speed** can either be left at the default 115200 value or set to the maximum capability of your modem.

If the WAN 2 port is being set up to make a call, enter the telephone number to be dialed in the **Dial Number** field.

If the WAN 2 port is being set up to answer a call, click the **Answering** option (the Dial Number field becomes inactive).

24. Click **OK** when you are satisfied with your selections.
25. The **Default T1 Parameters** dialog box is displayed.



Set the **T1 Framing Format** to match that of your T1 Service provider.

The **D4** Framing Format is a 193-bit frame format that uses the 193rd-bit for framing and signaling information. The D4 Framing Format uses 12 frames.

The Extended SuperFrame (**ESF**) Framing Format uses 24 frames and provides CRC error detection and 4Khz Facility Data Link (FDL).

26. Set the **T1 Line Coding** to match that of your T1 Service provider.

    The Alternate Mark Inversion (**AMI**) Line Coding is a bipolar coding scheme in which successive ones alternate in polarity to prevent a BiPolar Violation (BPV). A BPV occurs when two consecutive ones are the same polarity.

    The **B8ZS** Line Coding technique is used to satisfy the ones density requirements of the T1 carrier facilities while also allowing clear channel data. Since the system timing is recovered from the pulse width of the ones, it is important to ensure that there is an adequate proportion of ones in the data stream. If the data stream contains more than 8 consecutive zeros - a condition that could disrupt system timing - B8ZS substitutes a predetermined pattern for the zeroes. This substitution intentionally causes a BPV to occur, alerting the unit on the receiving end that a substitution has taken place.

27. Set the **T1 Line Type and Length** for either a short haul line type or long haul line type.

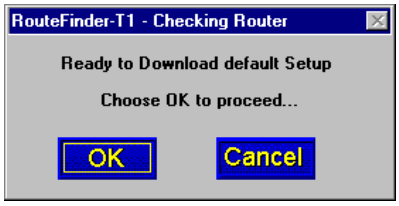
    The long haul line type is **CSU (0db) or DSX-1 (0-133ft)** option which is also the default. CSU allows the DSX-1 signal to be transmitted up to 6000 feet at Line Build Out (LBO) options of 7.5db, 15db, or 22.5db.

    The DSX-1 is a short haul line type often referred to as “Cross-connect” within the telco central office. The DSX-1 is available in 5 ranges up to 655 feet.

28. Set the **T1 Channel Allocations** for the number of channels assigned by the local T1 Service provider. If a full T1 service is provided (e.g., 24 channels), then use the default and click **OK** to continue.

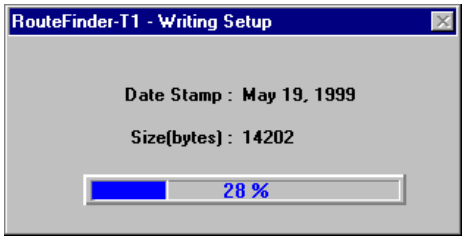
    If a fractional T1 service is provided, then click on each channel that is not in service and then click **OK** to continue.

29. The **Checking Router** dialog box is displayed.

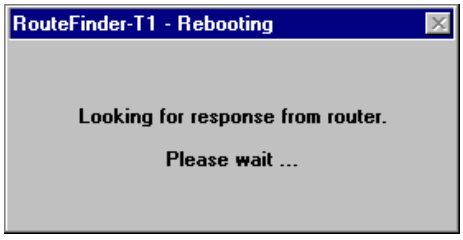


Click **OK**.

30. The **Writing Setup** dialog box (with the current date and the file size in bytes) is displayed as the software sends the configuration file to the RouteFinder.



31. Next, the **Rebooting** dialog box is displayed.



Check to ensure that the **Boot** LED on the RouteFinder goes Off after the download is complete and the RouteFinder is rebooted (the **Rebooting** dialog box goes away).

32. You are returned to the Multi-Tech Installation CD screen where you can now install (on your PC's hard drive) either Acrobat Reader (by clicking the Acrobat Reader icon) or the User Guide (by clicking the Install Manuals icon).

33. At this time your RouteFinder is operational.

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 4 - RouteFinder Software

MultiTech® Systems

Introduction

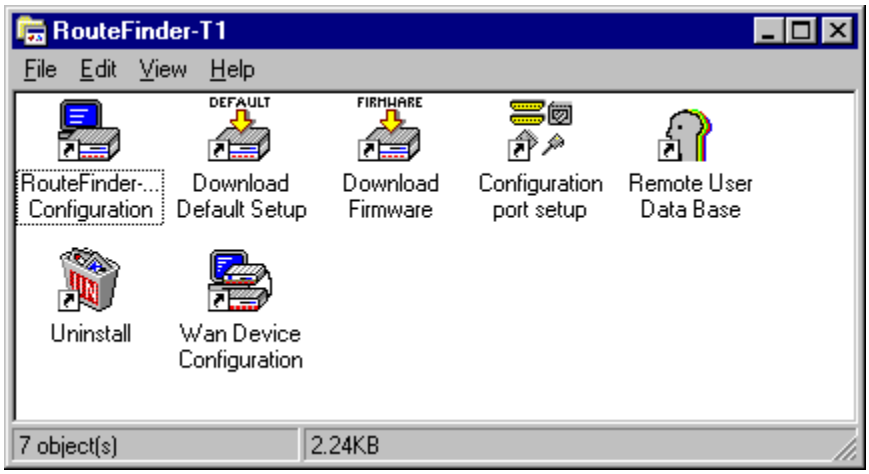
This chapter describes how to make changes in the configuration of the RouteFinder's software and discusses the impact of the changes. The major configuration parameters were set during the loading of the software (Chapter 3). The RouteFinder software and configuration utilities allow you to make changes to the initial configuration.

The **RouteFinder Configuration** utility enables you to setup and configure various parameters of the RouteFinder's protocol stacks and device drivers. You also have the option to perform basic hardware testing and run the console terminal from this menu.

The other six utilities provide additional functionality. The **Download Default Setup** utility allows you to download the default settings, configured during installation, to the RouteFinder. If you are installing for the first time, you will download this setup at the end of the installation before operating the RouteFinder. If you have made changes to the RouteFinder Configuration and now want to revert to the default setup, you can do so through the RouteFinder program group. The **Download firmware** utility enables you to download the firmware to the RouteFinder. This may be necessary in the case of repair or upgrade. The **Configuration port setup** utility allows you to change the method by which you access your RouteFinder. You can establish a direct connection, a PC to the Command port, or through your network connection to the LAN port. The **WAN Device Configuration** utility opens the Print Console, a terminal emulation program that enables configuration of external devices connected to the WAN 2 port. The **Remote User Data Base** utility (supported through the Command port) allows you to establish and maintain a database of information about your remote users. You can add and remove remote users, or edit existing user information in the database. Remote User Data Base is supported only if WAN 2 is configured for a Dial-in application (Refer to Appendix D for the procedure). The **Uninstall** utility enables you to completely remove all the components of the RouteFinder-T1 program group.

Before You Begin

Your RouteFinder -T1 program group contains several utility programs that provide the maximum flexibility for configuration and use. These utilities are accessible in Windows by clicking **Start | Programs | RouteFinder-T1 | (*utility*)**.



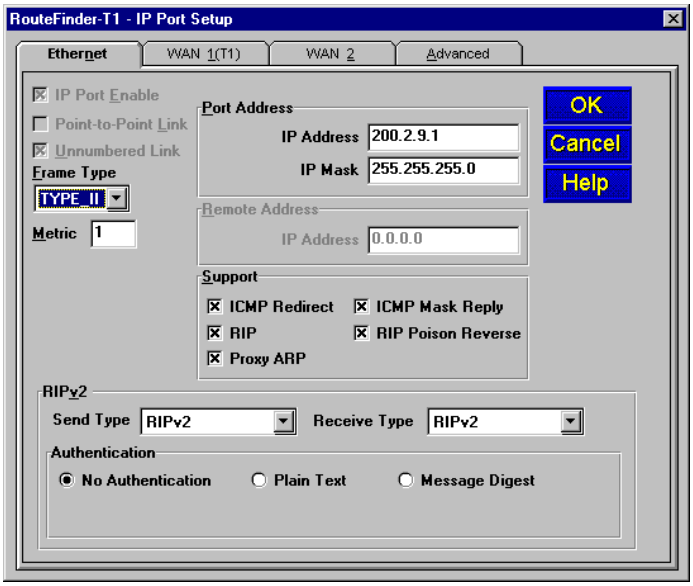
Router Configuration

The **RouterFinder-T1 Router Setup** menu has 14 buttons (two rows of five buttons plus one row with four buttons) that enable you to display and change the protocol stacks, define the output of the RouteFinder, perform network management functions, test the communications link, print messages received from the target RouteFinder, and download setup information to the RouteFinder.

Three buttons in the bottom row open the Statistics feature, open the on-line Help system, and end (Exit) a RouteFinder Setup session.

IP Port Setup

The **IP Port Setup** dialog box allows you to change the IP routing capabilities that were established during the software installation. This dialog box contains four tabs: Ethernet, WAN 1 (T1), WAN 2, and Advanced.



The **Unnumbered Link** option can be selected (checked) for the WAN ports for point-to-point links. When selected, it disables the Port Address and Remote Address groups. Unnumbered links are useful only between two routers; in this case, local and remote. When running RIP over a PPP link, both ends of the link must be either unnumbered or numbered with the same IP subnet. An advantage of not assigning an IP address to each WAN port is that you conserve valuable network and subnet numbers.

The **Remote IP Address** defines the IP address for the destination end of a point-to-point link and is necessary only of the selected WAN port has been enabled for point-to-point operation.

Note: the remote IP address must fall within the same IP network as the local IP address.

The **Frame Type** option defines the MAC layer frame encapsulation to be used for IP transmissions from the specified port. The Ethernet port supports Type II and SNAP frames, but the WAN ports support only Type II frames.

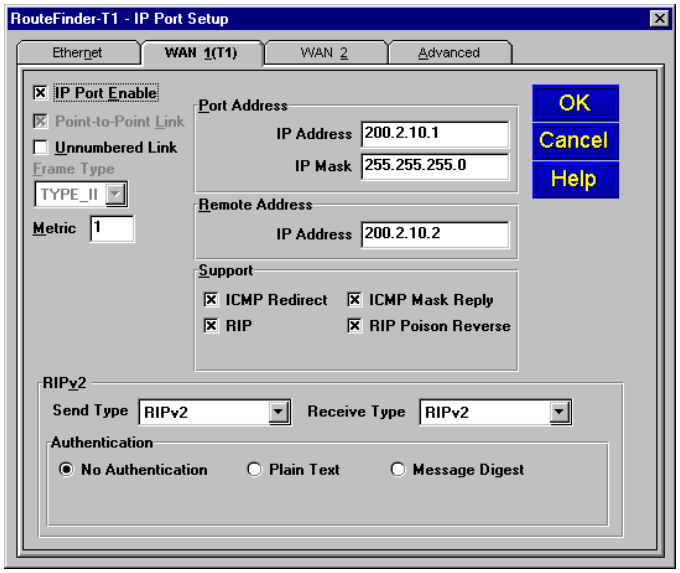
In the **Support** group, **ICMP Redirect** defines if the specified port is permitted to issue an ICMP Redirect message to the source IP address. The most likely cause of this message is the delivery of a datagram to a router that is not on the forwarding path to the destination address. This is often due to a wrong configuration of the IP client sending the datagram. The packet causing the ICMP Redirect message to be transmitted is forwarded to the appropriate router.

ICMP Mask Reply enables support for nodes on the connected networks to learn their subnet masks.

RIP enables RIP based routing on the specified port, and is normally enabled. However, RIP can be disabled if you are using WAN links in Dial-on-Demand mode. In such links, disabling RIP will reduce traffic on the link as this will also disable periodic RIP broadcasts. RIP routing on the port will be automatically turned off when Dial-on-Demand is enabled in PPP port setup.

Finally, the **RIP Poisoned Reverse** option defines if Poisoned Reverse RIP messages are supported on the specified port. Generation and processing of poisoned routes (RIP entries with their respective metric set to 16 (defined as infinity) is enabled/disabled by this parameter. Poisoned reverse is a method used by RIP to improve the rate of convergence of the routing tables of interconnected IP routers. Routers supporting poisoned reverse that receive such RIPs ignore the entries set to 16 and thus prevent the propagation of unnecessary information (often incorrect when a topology change occurs) which in turn speeds up the rate at which RIP will correctly map the current network topology.

The **Ethernet**, **WAN 1 (T1)** and **WAN 2** tabs allow you to configure parameters for the selected port. Although these tabs all contain the same option groups, certain parameters may be inactive or disabled (grayed-out) when they do not apply to the selected port.



RIPv2 packet setup is accomplished at the bottom of the Ethernet and WAN port tabs. The **RIPv2** group enables you to set up the send and receive packet types as either RIPv2 (default), RIPv1 Compatible, or None. You can also set up RIPv2 authentication here.

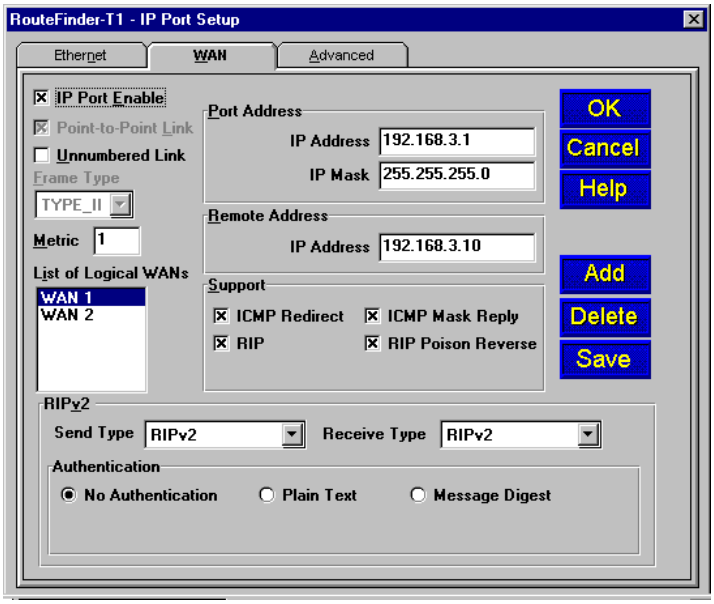
Routing Information Protocol, Version 2 (RIPv2) has enhanced “explicit” netmask information and supports several new features including external route tags, subnet masks, next-hop addresses, and authentication. Subnet mask information makes RIP more useful in a variety of environments and allows the use of variable subnet masks on the network. Support for next-hop addresses permits the

optimization of routes in an environment that uses multiple routing protocols. For example, when RIPv2 is being run on a network along with another IGP, and one router is running both protocols, then that router can indicate to the other RIPv2 routers that a better next-hop than itself exists for a given destination.

The **Authentication** group is the RIPv2 mechanism for authenticating the sender of the routing eliminates the vulnerability of the routing infrastructure. This authentication scheme is essentially the same mechanism provided by OSPF. Currently, only a plain-text password is defined for authentication.

For **Plain Text** RIPv2 authentication, the maximum length of the password is 16 characters; however, Message Digest authentication can have a key id field of up to 50 characters.

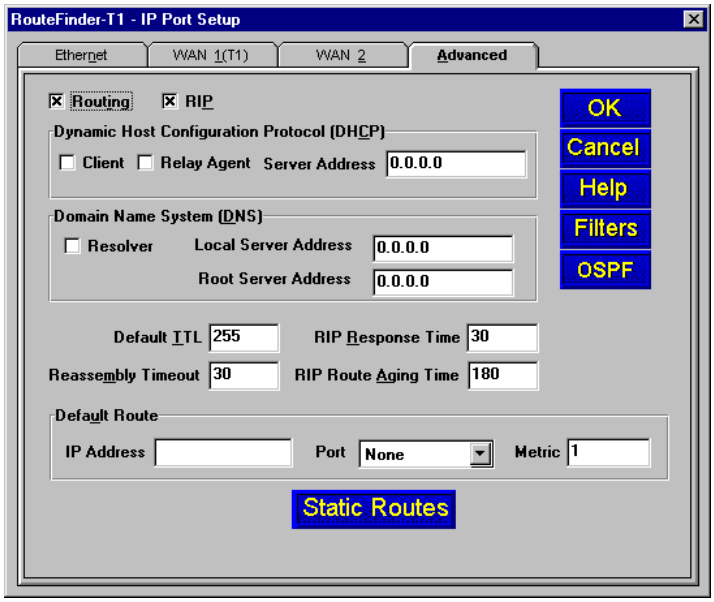
If the RouteFinder is configured for Frame Relay, the **IP Port Setup** dialog box displays a single WAN tab. Logical WANs are established in this dialog box and are mapped to DLCIs in the **Frame Relay DLCI** dialog box. Mapping DLCIs to logical WANs using IP requires an IP Address and IP Mask in the Port Address group; and, it requires an IP Address in the Remote Address group. When assigning IP addresses, the Port Address and Remote Address must be in the same network segment.



To add logical WANs in a frame relay configuration, click the **Add** button and the next WAN number is displayed in the List of Logical WANs window. Make the appropriate Port Address and Remote Address assignments and click **Save**. You can also edit a logical WAN address by clicking on the logical WAN in the List of Logical WANs window, changing the Port Address and Remote Address assignments and clicking **Save**. To delete a logical WAN, highlight the WAN number in the List of Logical WANs and click the **Delete** button.

Once the logical WANs are established, you must go to the **Frame Relay DLCI** dialog box to map the logical WANs to a DLCI.

The **Advanced** tab controls the timers, Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) options, the default route, Filters, OSPF, and Static Routes.



In most cases, you should not have to change any of the timers (i.e., default TTL, Reassembly Timeout, RIP Response Time, and RIP Route Aging Time). The DNS Resolver is supplied for remote Telnet clients when the router is configured for remote access and the terminal server application is enabled.

The **Routing** option is normally enabled (checked); however, if you do not wish to have IP packets routed, then uncheck this item. If IP routing is disabled and bridging is enabled, IP packets are bridged; i.e., IP packets are transferred. Bridging would be more appropriate in a situation where you are Internet-connected and don't have a large number of IP addresses.

The **RIP** option enables RIP-based routing. RIP (Routing Information Protocol) is a protocol used among routers to exchange routing table information. RIP is the most common protocol used in both IP and IPX networks. It is also used internally by client workstations in IPX networks to obtain routes (shortest, or otherwise) to any distant network. RIP-based routing should normally be enabled (checked) . It can be disabled, however, if you are using WAN links in Dial on Demand (DOD) mode. For DOD links, disabling RIP will reduce traffic on the link and it will also disable periodic RIP broadcasts. RIP routing on a given port will be automatically turned off when DOD is enabled on the PPP Port Setup tab for the WAN port.

The **Dynamic Host Configuration Protocol (DHCP)** group enables you to set up the WAN ports as client-only. In this case, a PPP client connected to the WAN port will be on the same IP network as the LAN port of the RouteFinder. This feature can save some extra IP addresses that otherwise would have been taken up by the WAN port. Enabling the Client option allows the RouteFinder to dynamically get an IP address for a PPP client coming up on its "Client-only" WAN port. When this option is enabled, there must be a DHCP server or a DHCP relay agent on the connected LAN in order for the RouteFinder to acquire an appropriate IP address.

In most cases, you should not have to change any of the timers (i.e., Default TTL, Reassembly Timeout, RIP Response Time and RIP Route Aging Time). The **Domain Name System (DNS)** Resolver is supplied for remote Telnet clients when the router is configured for remote access and the terminal server application is enabled.

A brief description of OSPF is provided in the following section. For details on other parameters, refer to the online **Help** provided with your RouteFinder software.

Open Shortest Path First (OSPF)

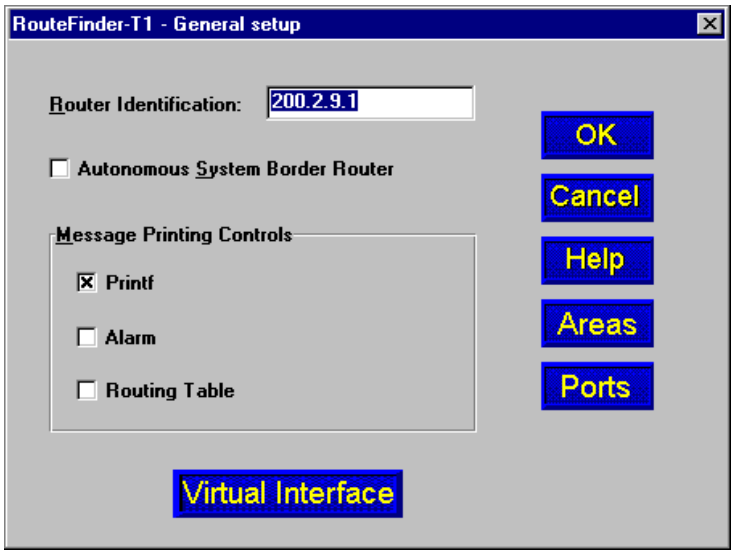
Open Shortest Path First (OSPF) is a common TCP/IP routing protocol that provides robust and efficient routing support in the most demanding Internet environments. OSPF calculates routes using the number of routers, the transmission speed, expected delays, and the cost of the route. Version 2 of the OSPF protocol is designed to be run internal to a single Autonomous System. Each OSPF router maintains an identical database describing the topology of the Autonomous System. From this database, a routing table is calculated by constructing a “shortest-path” tree.

OSPF recalculates routes quickly in the event of topological changes using a minimum of routing protocol traffic.

Under OSPF, networks can be grouped together into “areas,” each of which is the generalization of an IP subnetted network. The topology of an area is hidden from the rest of the Autonomous System. The result is that information hiding enables a significant reduction in routing traffic. Also, routing within an area is determined only by the area’s own topology, protecting the area from “bad” routing data.

All OSPF protocol exchanges are authenticated; i.e., only trusted routers can participate in the Autonomous System’s routing. Furthermore, a variety of authentication schemes can be used; in fact, separate authentication schemes can be configured for each IP subnet.

Click the **OSPF** button on the **Advanced** tab to open the **General Setup** dialog box.



The **Router Identification** field defines the IP address of the router.

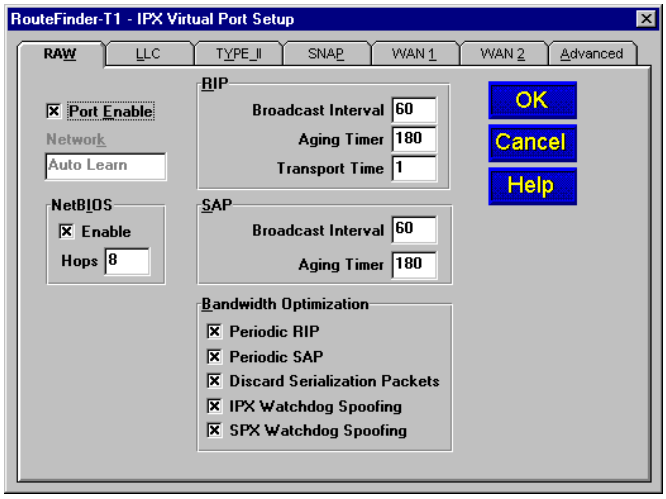
The **Autonomous System Border Router** feature enables the RouteFinder as an Autonomous System (AS) border router, capable of exchanging routing information with routers in other autonomous systems. The AS border router then advertises external routes throughout its autonomous systems. By default, this option is disabled (unchecked).

Items in the **Message Printing Controls** group can be enabled to generate messages in the RouteFinder’s built-in terminal application. While these are helpful tools for diagnostics and trouble shooting, they are generally left disabled (unchecked) to avoid possible degradation of router performance. The Printf feature enables generation of print messages, the Alarm feature enables generation of Alarm messages, and the Routing Table feature enables generation of messages relating to the Routing Table used by IP and IPX routers.

The **Areas** button opens the **Area Setup** dialog box used to configure various parameters for OSPF areas; The **Ports** button opens the **OSPF Port Setup** dialog box used to configure various parameters relating to the OSPF ports; and, the **Virtual Interface** button opens the **Virtual Interfaces** dialog box through which you can add, edit, and remove virtual interfaces.

IPX Setup

The **IPX Virtual Port Setup** dialog box controls the four frame types and set up the two WAN ports. The Advanced tab enables IPX routing, Auto Learn of Ethernet Network Numbers, and the distributed name of the RouteFinder can be designated or changed.



In IPX based networks using Ethernet, LAN segments can support the use of four different Ethernet frame formats (RAW, LLC, TYPE_II, and SNAP) over the same physical link provided each frame type has a unique network address as a virtual port.

NetBIOS, when enabled, enables the transport of Novell encapsulated NetBIOS packets on the specified virtual IPX port. Refer to Novell documentation regarding NetBIOS operation over NetWare based LANs. The Hops text box defines the distance, in hops, for the routing of Novell encapsulated NetBIOS frames on the specified virtual IPX port, and the recommended value is 8.

Periodic RIP (Routing Information Protocol) refers to broadcasts transmitted from the RIP virtual IPX port at a given frequency so all routers on the internetwork maintain consistent routing tables. Increasing the frequency of RIP broadcasts can consume excessive bandwidth, especially on low-speed WAN links. Sixty seconds is the recommended interval between RIP broadcasts.

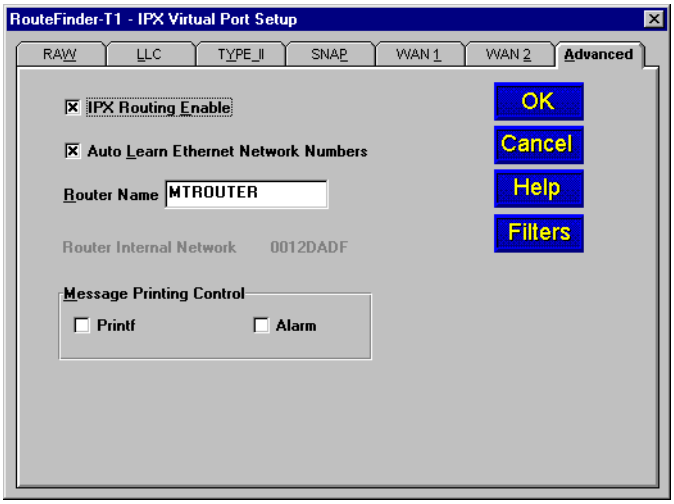
Periodic SAP (Service Advertisement Protocol) is used in IPX based networks to allow servers (application servers, file servers, print servers, communication servers, etc.) to advertise their presence on the internetwork. Routers use these advertisements to build up tables listing the servers so they can then advertise these servers on the local segments and provide routers to the server. Client workstations can request a list of these servers from the router.

Discard Serialization Packets, when enabled (checked), causes the IPX router to discard Novell NetWare File Server serialization security frames received from the specified virtual IPX port. Novell NetWare File Servers implement broadcast frames, often referred to as security frames, that contain serialization information regarding the license of the file server executable. This feature permits filtering of these broadcasts to help reduce WAN traffic and is not intended to interfere with copyright protection mechanisms. This feature is automatically turned on when Dial-On-Demand is enabled in PPP port setup.

The default RIP and SAP timer settings should work for most applications. Under certain circumstances, disabling IPX and SPX Watchdog Spoofing in the Bandwidth Optimization group has proven effective.

The two IPX WAN Setup dialog boxes allow you to enable or disable IPX routing on the WAN ports, change the network numbers for the WAN ports, change the default RIP and SAP timers, and optimize the bandwidth. The IPX WAN network number has to be the same on both ends of the link and must be unique throughout the internetwork. If a WAN port is configured in a point-to-point operation, both WAN network numbers have to be the same and unique.

The **Advanced** tab contains options which control the routing of the protocol, enable auto learn of Ethernet network numbers, define the broadcast name of the RouteFinder, and control IPX filtering.



If bridging of IPX packets is desired, IPX routing must be disabled and frame type support for the frame type must be enabled. Bridging consumes more bandwidth; therefore, it should be used only when required. For example, if all workstations are required to be on the same network operating system (same backbone) then bridging should be used.

If there is a server on the local segment, then IPX network number auto learn should be enabled. If there is no server, or if for some reason the router comes up before the server, the router will default to some random network numbers after a short period of time.

The **IPX Routing Enable** feature enables IPX routing. By default, IPX routing is enabled (checked). If you disable (uncheck) this feature, but have Spanning Tree Bridging enabled, IPX packets are bridged. If you disable this feature and disable Spanning Tree Bridging, IPX packets are dropped.

The **Auto Learn Ethernet Network Numbers** feature means that the RouteFinder can automatically learn the IPX network numbers set up on the Ethernet from a Novell file server (or any other server, including routers that support SAP). If you have a file server on the LAN side, you can use this feature. By default this feature is enabled. By disabling this feature you can decrease the amount of traffic that the Router must learn. In such cases, it would be best for the network administrator to hard code the network numbers.

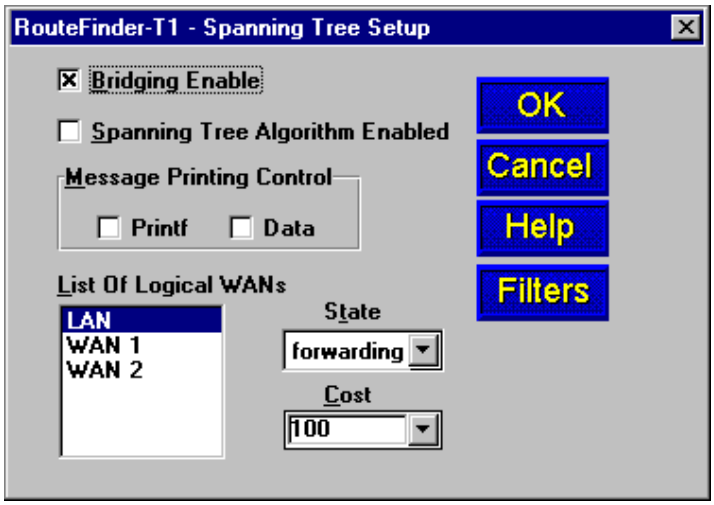
The **Router Name** field defines the text name for the IPX router that is distributed to the other IPX services via SAP messages. This name can be up to 48 characters in length. The **Router Internal Network** feature displays a network number for a virtual LAN within the RouteFinder. This number is provided for Novell compatibility. Novell file servers define a similar virtual network number upon which the actual file server node resides in order to ensure that the file server remains equidistant from all other services located on the attached IPX networks. The RouteFinder assumes the Ethernet port address's least significant 4 bytes for this value. In case this value clashes with any of your IPC internetwork values, contact Multi-Tech technical support for advice.

The **Message Printing Control Group (IPX)** feature controls the display of various messages on the console terminal. These messages can be a useful tool for troubleshooting and diagnostics. Normally however, these items should be disabled (unchecked) to avoid a possible degradation of router performance. The **Printf** feature enables generation of IPX print messages and the **Alarm** feature enables generation of IPX alarm messages.

The **Filters** button (IPX) displays the IPX **Filtering Setup** dialog box used to add, edit and remove IPX filters from the filtering database.

Spanning Tree Setup

When Bridging is enabled, the **Spanning Tree Setup** dialog box controls simple transparent bridging between two remote Ethernet LANs. However, if your internetwork contains any loops or redundant links, then the Spanning Tree algorithm must also be enabled. If you use only the IP and IPX protocols, leave bridging disabled to allow the RouteFinder to operate more efficiently.



The RouteFinder defaults with transparent bridging enabled on all ports. In most applications, the *forwarding* state should be enabled. When required, the RouteFinder will make the transition from blocking to forwarding automatically.

The **Message Printing Control** group allows the RouteFinder to display messages in the console terminal for the port highlighted in the List of Logical WANs. These messages can be useful as a troubleshooting and diagnostic tool, but are disabled by default. Normally, all items should be disabled to avoid a possible degradation of router performance. Options in this group include: a **Printf** feature which enables generation of print messages; and, a **Data** feature that enables generation of data messages.

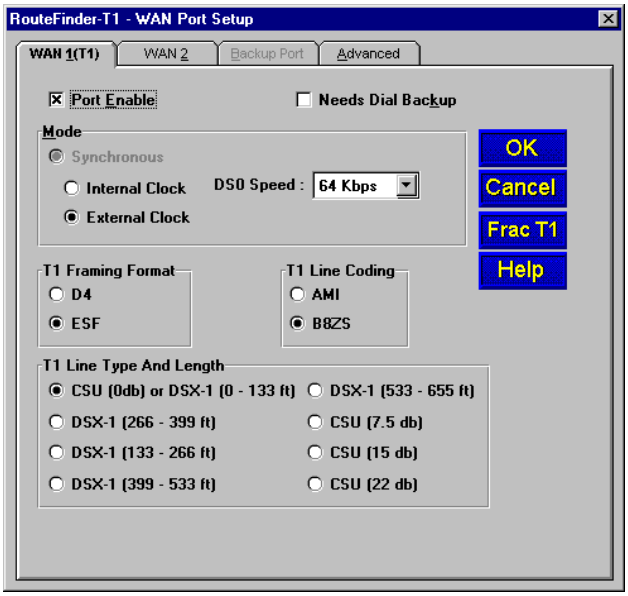
The **Filters** button opens the Spanning Tree Filtering dialog used to add, edit and remove filters in the filtering database.

WAN Port Setup

The **WAN Port Setup** dialog box allows you to configure various parameters for the WAN connections including T1 Framing Format and line coding for WAN1, mode and connection method for WAN 2, Backup port if WAN 2 is to be used for dial backup, and the Advanced tab. The three tabs labeled WAN 1(T1), WAN 2, and Backup Port are used to configure their respective ports, and the Advanced tab is used to enable features for all three ports.

The **Port Enable** feature enables routing and bridging on the selected WAN port. The RouteFinder is capable of dialing a backup number in case WAN 1(T1) looses its connection (i.e., carrier signal is dropped). If WAN 1 needs backup, then WAN 2 is used for this purpose and cannot be used for routing. When **Needs Dial Backup** is enabled (checked), the WAN 2 tab becomes inactive (grayed-out), and the Backup Port tab becomes active. You must enter a dial backup number in the Backup Parameters for WAN 1 group on the Backup Port tab.

WAN 1(T1) Configuration



The **Mode** group for the WAN 1(T1) link is always in synchronous mode. You must configure clocking using the appropriate option. By default, **External Clock** is enabled. This means that the clocking will be supplied by your T1 service provider. If **Internal Clock** is enabled, it means that the RouteFinder will supply the clocking to the T1 facility. When Internal Clock is enabled (checked) you must also set the Clock Speed. Use the drop-down list to select the Clock Speed for the WAN 1 port.

The **T1 Framing Format** group is used to match the T1 framing format to that of your T1 service provider. The options include **D4** framing (12 frames), a 193-bit frame format that uses the 193rd bit for framing and signaling information; and, **ESF** – Extended Super Frame (ESF) framing (24 frames) that provides Checksum (CRC) error detection and 4KHz Facility Data Link (FDL). The T1 Framing Format information is provided by your T1 service provider.

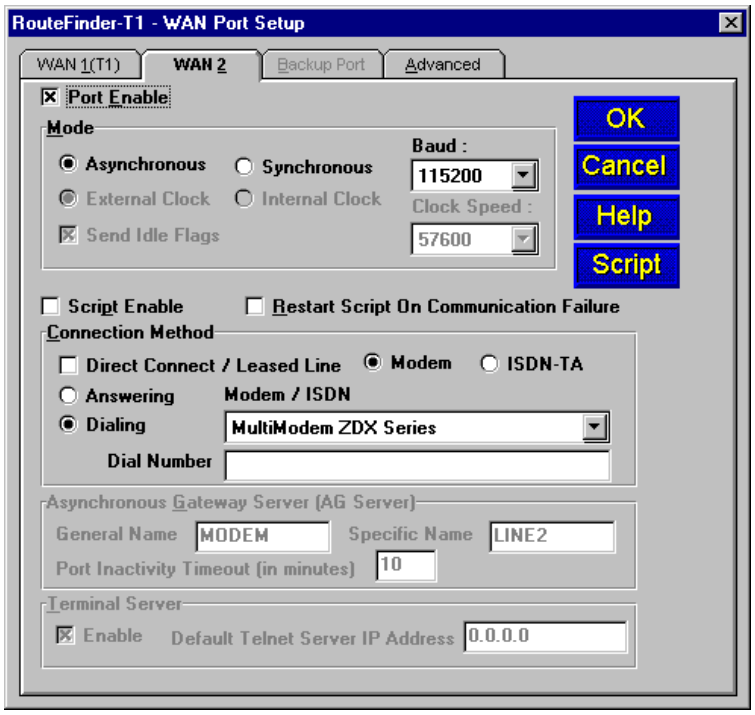
The **T1 Line Coding** group is used to match the T1 Line Coding type to that of your T1 service provider. **AMI** (Alternate Mark Inversion) line coding is a bipolar coding scheme in which successive ones alternate in polarity to prevent a BiPolar Violation (BPV). A BPV occurs when two consecutive ones are the same polarity. **B8ZS** (Binary 8 Zero Suppression) line coding is used to satisfy the ones density requirements of the T1 carrier facilities, while also allowing clear channel data. Since the system timing is recovered from the pulse width of the ones, it is important to ensure that there is an adequate proportion of ones in the data stream. If the data stream contains more than eight consecutive zeros – a condition that could disrupt system timing – B8ZS substitutes a predetermined pattern for the zeros. This substitution intentionally causes a BPV to occur, alerting the unit on the receiving end that a substitution has taken place.

The **T1 Line Type and Length** group is used to set the type and length of the T1 line. The line can be set up as either a short haul line or a long haul line. The default setting is CSU (0db) or DSX-1 (0-133ft), which is a long haul line type. **CSU** allows the DSX-1 signal to be transmitted up to 6000 feet at Line Build Out (LBO) options of 7.5db, 15db, or 22.5db. **DSX-1** is a short haul line type often referred to as “Cross-connect” within the telco central office. The DSX-1 is available in 5 ranges, up to 655 feet.

The **Frac T1** button opens the DSO Allocations dialog used to configure Fractional T1 parameters. Select the DSOs that correspond to the range of DSOs supplied by your T1 service provider. If your T1 service provider has your line configured for DSOs 1 through 10 and 20 through 24, you should disable (unchecked) all the DSOs that do not fall into the two ranges (11 through 19 should be disabled).

WAN 2 Configuration

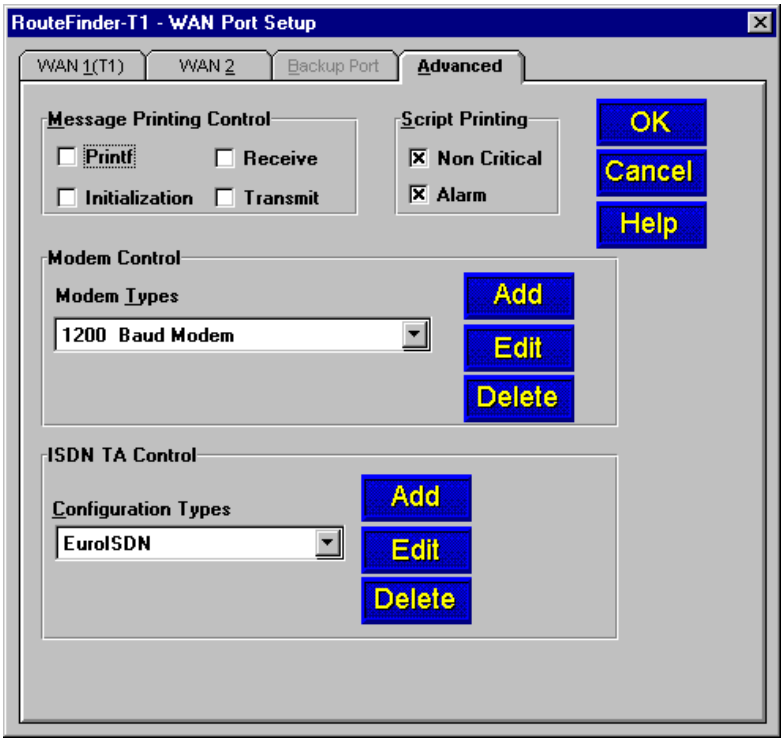
The WAN Port Setup dialog box for WAN 2 controls how the port is configured (i.e., frame relay or point-to-point). If WAN 2 is configured for frame relay, then the mode of the port is synchronous. If the port is configured for point-to-point, then the mode can be either synchronous or asynchronous. If the mode is asynchronous, then the connection method can be either Answering or Dialing. If the connection method is dialing, then a number to be dialed has to be entered in the Dial Number field and the Modem Types field.



Three connection methods are available for WAN 2: either Direct Connect / Leased Line, Modem, or ISDN-TA. WAN 2 defaults to a Modem connection and you can select another modem from the drop-down list if you aren’t connected to a MultiModem ZDX Series modem. If this is the dialing end of a dial-up link, you will need to enter the phone number to be dialed in the Dial Number text box in the **Connection Method** group.

If the WAN 2 port is configured for an Asynchronous mode of operation and Scripting is required, you can enable Scripting by checking the **Script Enable** option. Scripting allows special handling of the port (e.g., extra authentication, special communications equipment, etc.). You can also enable **Restart Script On Communication Failure** by clicking (checked) the box. By clicking on the **Script** button, you can also compile a new script, edit an existing script, and download your script. A list of Script commands by function and an example of a typical script is provided in Appendix B.

The WAN Port Setup **Advanced** tab contains options which control message printing and script printing, modem type control, and ISDN TA control.



The **Message Printing Control** group allows you to enable items that you want to be displayed on console messages. These messages can be useful as diagnostic and troubleshooting tools but should remain disabled (unchecked) under normal circumstances to avoid possible degradation of router performance.

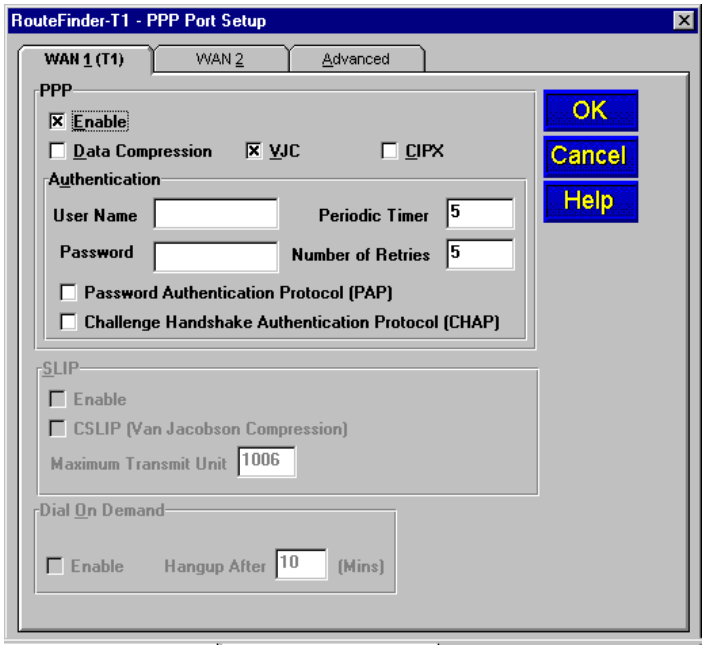
The **Script Printing** group allows script printing on the WAN 2 port during non-critical periods and during alarm situations. Both these features are enabled by default. A list of Script commands by function and an example of a typical script is found in Appendix B - Script Commands.

The **Modem Control** group applies only to WAN 2 and allows you to select a new modem from the drop-down list. Add, Edit, and Delete buttons allow you to add new modems, make changes to existing modems, or remove an existing modem from the list.

The **ISDN TA Control** group applies only to WAN 2 and allows to select commonly used, pre-configured ISDN configurations from the drop-down list. Add, Edit, and Delete buttons allow you to add a new ISDN configuration, make changes to an existing configuration, or remove an ISDN configuration from the list.

Point-to-Point Setup

The **PPP Port Setup** dialog box controls the WAN port protocol and dial on demand (DOD). The WAN port protocol can be either Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP). Of these two protocols, PPP is the more robust as it allows the end-points to negotiate the use of the link and protocol parameters in a standardized way and also allows for standardized encapsulation of the packets. SLIP is an older protocol which requires manual authentication using a script.



PPP is the default protocol.

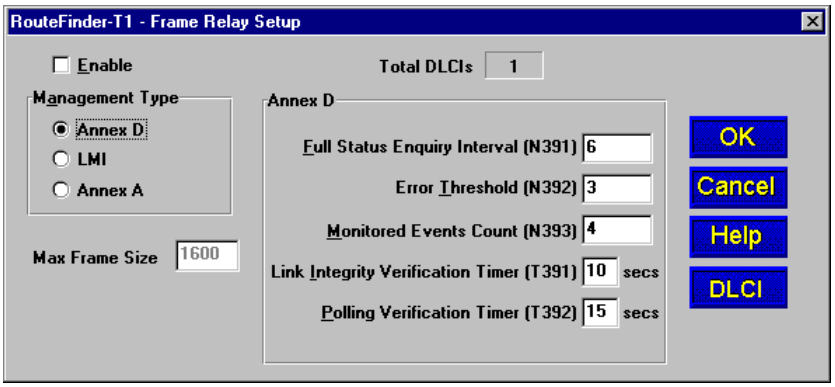
If WAN 1(T1), SLIP and Dial On Demand are inactive. If WAN 2 and SLIP is being used, click the PPP Enable option to disable PPP, then click the SLIP Enable option. Determine if the TCP header is going to be compressed using VJC compression. If VJC compression is used, click the CSLIP (Van Jacobson Compression) option.

The Point-to-Point **Advanced** tab contains options which control echo request, message printing, and termination and configuration requests.

Frame Relay Setup

The **Frame Relay Setup** dialog box displays the Management Type, details of that management type, and the number of DLCIs that are active. Frame Relay parameters have to be set up exactly as they are provisioned from the network service. Therefore, it is important not to change any Frame Relay parameters; and, when adding new DLCIs that they agree with the way your frame relay service is provisioned.

Note: When Frame Relay Service is employed by the Telco, the Frame Relay enable option must be checked and your Frame Relay parameters must be configured (e.g., Management Type and DLCIs provided by Telco).



In the **Frame Relay Setup** dialog box, you can change the Management Type by choosing one of the three options and then the detail parameters for that option are displayed to the right of the Management Type. For example, Annex D (See above) is the chosen management type with the Full Status Enquiry Interval [N391] set to 6 down through Polling Verification Timer [T392] set to 15.

Occasionally the Management Type parameters may need to be changed to correct a problem. In these cases making the following changes (aaplicable to Annex D) could alleviate the problem:

1. Change the **Link Integrity Verification Timer**. This feature sets how often the RouteFinder verifies that the link is good. Changing the setting from the default value of 10 seconds, to a lower value; e.g., 5 seconds, will increase the frequency of those verifications.

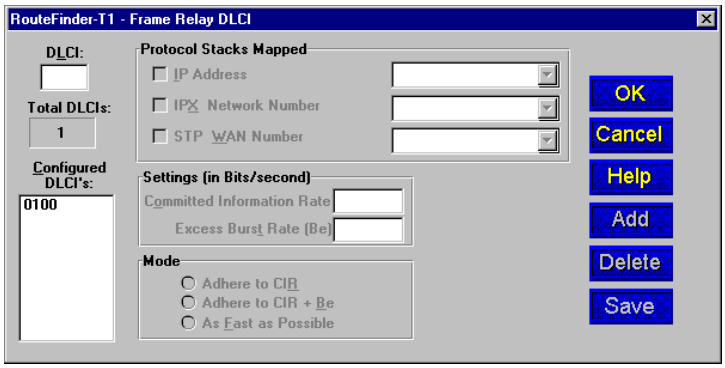
2. Change the **Full Status Enquiry Interval** to affect how often DCLI Status is updated. This parameter defines how often the RouteFinder will send a request for DLCI status information along with the Link Integrity Verification request. The default value includes such a request every sixth time the link integrity is checked. A value less than every sixth request will allow faster detection of active/inactive DLCIs, but will also produce a slight increase in management overhead.

3. Change the **Monitored Events Count** and the **Error Threshold** to affect the RouteFinder's sensitivity to errors on the link. Every management frame received by the RouteFinder is considered an event, and if the link integrity sequence numbers are wrong, for example, it is considered an "errored" event. With the default settings, if **Error Threshold** is 3 and **Monitored Events Count** is 4, and 3 out of 4 events are "errored", then the link is considered to be bad, and the RouteFinder stops sending on all DLCIs and restarts the initial procedures to activate the link.

If you click the **DLCI** button, the Frame Relay DLCI dialog box is displayed.

Frame Relay DLCI

The **Frame Relay DLCI** dialog box initially displays one DLCI in the total DLCI's window. This DLCI is provided as an example of a DLCI and has not been mapped to any protocol or logical WAN.



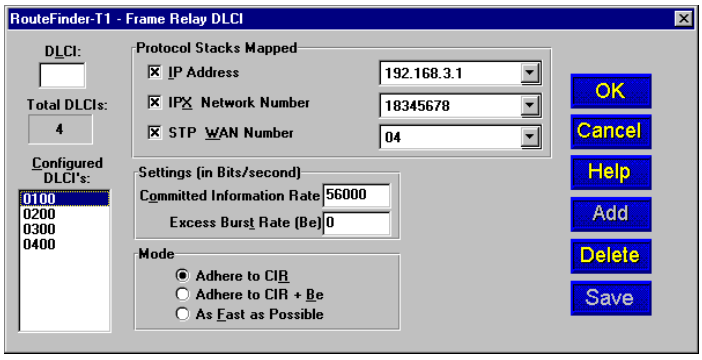
To add a new DLCI Number, enter the number in the **DLCI** window (e.g., 200). You do not have to enter the leading zeros. When you click the **Add** button, the new DLCI appears in the Configured DLCI's window. When you highlight the new DLCI, the default Committed Information Rate, Excess Burst rate of "0", and Mode setting of "Adhere to CIR" will be displayed.

You can now map the new DLCI to a protocol stack and frame relay parameters (i.e., CIR, Be, and Mode). To map a DLCI to a protocol stack, highlight the DLCI number in the Configured DLCI window. The **Protocol Stacks Mapped** group becomes active. Click on the protocol stack you wish to map the DLCI to and then click the down arrow for that protocol: address/network numbers for the protocol are displayed. Select the address/network number/STP WAN number you wish to map to the new DLCI. The protocol number that appears was established when you configured your logical WAN(s) for the selected protocol.

The frame relay parameters in the **Settings (in Bits/second)** and **Mode** groups have to coincide with how the frame relay access is provisioned. You will probably have to delete the default values and reenter your provisioned values that were provided by your T1 service provider.

The **Mode** settings are used to avoid possible loss of data. Mode settings determine how the RouteFinder handles congestion. The Mode group selects whether the RouteFinder should use its own throughput calculations to avoid congestion, or simply send data to the network As Fast as Possible. The RouteFinder calculates throughput after every CIR Measurement Interval, and can limit throughput to either the CIR (Adhere to CIR) or the CIR plus the Be (Adhere to CIR+Be).

The following Frame Relay DLCI dialog box illustrates DLCI 100 with all the protocol stacks enabled, their respective network numbers, and the default CIR, BE and Mode settings. You would map your DLCIs to your network protocols and set your CIR, Be, and Mode according to how your service provider set up your T1 service.



Once all DLCI's have been mapped, click **Save** and then click the **Download Setup** button on the **Router Setup** main menu to write the new DLCI configurations to the MTASR2-203 RouteFinder.

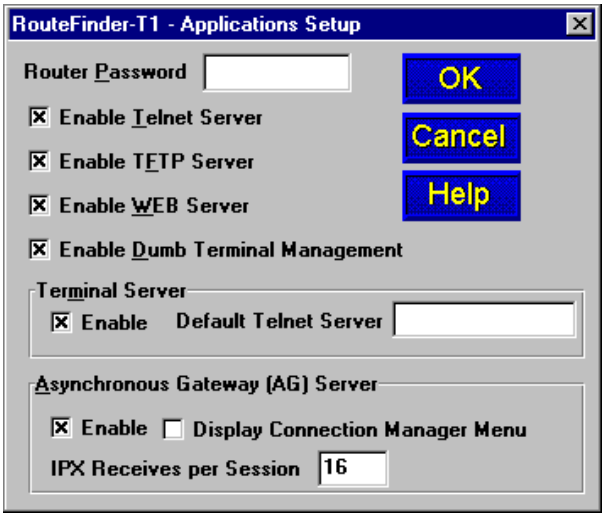
For more information on the Frame Relay DLCI dialog box, click the **Help** button.

Applications Setup

The **Applications Setup** dialog box lets you set up support for Telnet, TFTP (Trivial File Transfer Protocol), WEB, and Asynchronous Gateway servers in the RouteFinder. This dialog box is displayed by clicking **Others** on the Router Setup dialog box.

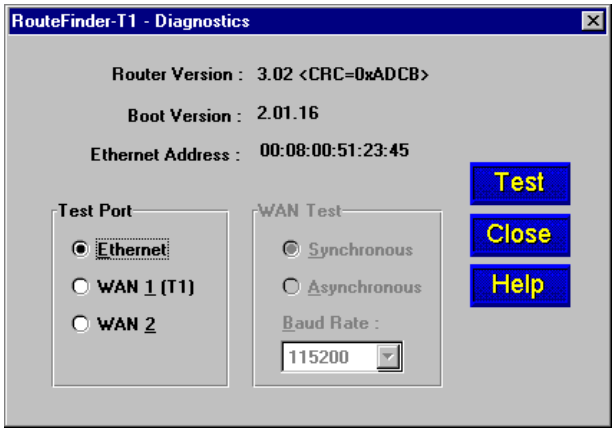
Telnet is an applications level protocol commonly found in IP-based networks that allow terminal emulation at a remote workstation. TFTP is a file transfer protocol that uses UDP and provides a simple method for transferring files between two nodes (one the server and the other the client).

The RouteFinder also supports Multi-Tech's Communications Services Interface (MCSI), Asynchronous Gateway server, or AG server or Netware Communications Services Interface (NCSI). In order to use this service every asynchronous communication line has a unique MCSI name across the internetwork.



Diagnostics

The RouteFinder is equipped with a built-in diagnostics utility that can be accessed through the COM port of your PC (remote users cannot access the diagnostics). Click **Built-in Test** on the **Router Setup** menu and the **Diagnostics** dialog box is displayed.



In the **Test Port** group, select the Ethernet, WAN 1(T1), or WAN 2 port and then click **Test** to start diagnostic testing.

For additional details and parameters about specific fields in the **Diagnostics** dialog box, click the **Help** button.

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 5 - Remote Configuration and Management

MultiTech® Systems

Introduction

This chapter provides procedures for viewing or changing the configuration of a remote unit. Two methods are provided to access a remote unit; the first method is modem based and the second method is using IP. Within the IP method, three applications can be used: 1) LAN-Based using TFTP (Trivial File Transfer Protocol), 2)Telnet as a client application, or 3) a standard web browser on the Internet.

Remote Configuration

Remote configuration requires the RouteFinder software to be loaded on the local PC. The local PC then controls the remote RouteFinder either via the modem connection or the LAN.

Modem-Based

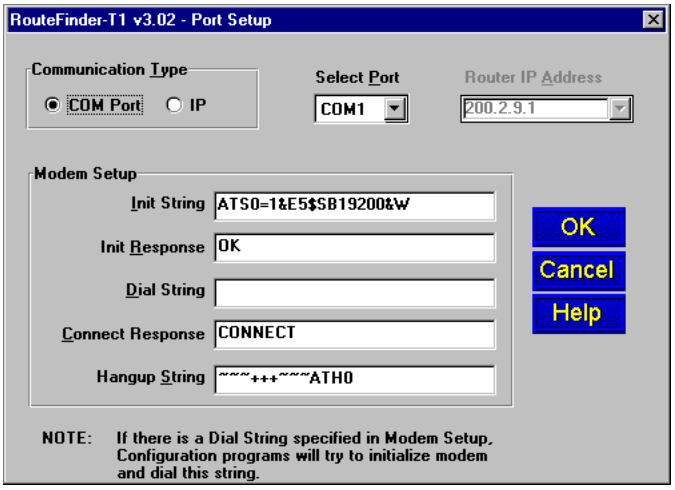
To remotely configure a RouteFinder, a local PC needs to be connected to a dial-up line and the RouteFinder software configured to call the remote RouteFinder. The remote RouteFinder needs to have a modem connected to a dial-up line and the Command Port. Once the connection to the remote unit is made, you can change the configuration as you see fit. Once the configuration is changed, you can down load the new configuration to the remote RouteFinder.

1. At the remote site, remove the serial cable from the PC to the Command Port connector on the back panel of the RouteFinder.
2. At the remote site, connect a special cable (Remote Configuration Cable) from the Command Port connector on the back panel of the RouteFinder to the RS-232 connector on the modem. The special cable is a serial cable with male connectors on both ends. Refer to Appendix A for cable details.

   Connect the modem to your local telephone line.

   Provide your telephone number to the person verifying your configuration.

   Configure the remote modem for 19200 baud and turn on Force DTR.
3. At the main site, connect your local PC to a modem that is connected to a dial-up line.
4. Install the RouteFinder software on the local PC. When installed, click **Start | Programs | RouteFinder | Configuration Port Setup**, or double click on the **Configuration Port** icon.
5. The **Port Setup** dialog box is displayed.



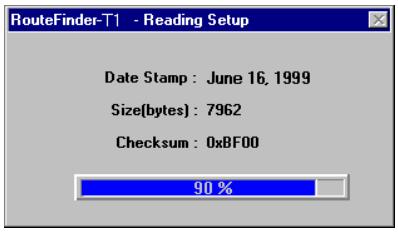
Verify that the **Communication Type** field is set for **COM port** and the **Select Port** field is set for the COM port of your local PC.

In the **Dial String** field, enter the AT command for dialing (ATDT) plus the phone number of the remote RouteFinder .

If your Modem Initialization String, Initialization Response, or Connect Response values are different from the defaults in the dialog box, refer to your modem user documentation and change the default values to match your modem.

Click **OK** when you are satisfied with all your selections.

6. Run the RouteFinder Configuration program. Click **Start** | **Programs** | **RouteFinder** | **RouteFinder Configuration**. or double click the **RouteFinder Configuration** icon in the RouteFinder program group.
7. The **Dialing Router** dialog box is displayed while software is dialing the remote RouteFinder.
8. Next, the **Reading Setup** dialog box is displayed.



9. The **Router Setup** dialog box is displayed. This is the dialog box of the remote RouteFinder. Refer to Chapter 4 for a description of each dialog box. For a detailed description of each field within a dialog box, refer to the on-line **Help** provided within your RouteFinder software.

10. After you have changed the configuration of the remote RouteFinder, click the **Download Setup** button to update the configuration. The remote RouteFinder will be brought down, the new configuration written to the unit, and the unit will reboot.
11. Click the **Exit** button when the downloading is complete.
12. The **Hangup connection with Router?** dialog box is displayed.

    Click **Yes** to disconnect the phone connection to the remote site.
13. If the same telephone number is **not** going to be used again in the immediate future, you may want to remove it from the **Port Setup** dialog box.
14. At the remote site, reconnect the RouteFinder to the serial port of the PC and from the Program Manager screen click the **Router Configuration** icon to verify that the RouteFinder is running.

LAN-Based

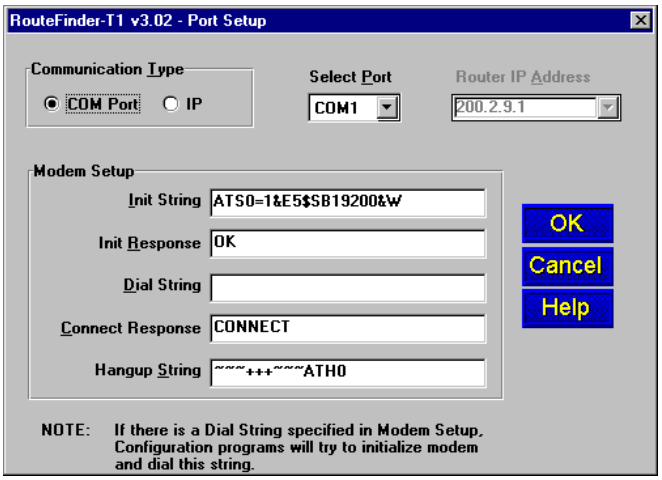
The LAN-based remote configuration requires a Windows Sockets compliant TCP/IP stack. TCP/IP protocol software must be installed and functional before the configuration program can be used.

1. You must assign an Internet (IP) address for the PC and for each node that will be managed by the configuration program. Refer to the protocol software documentation for instructions on how to set the IP addresses.

   Once you have completed this step, you should be able to use the protocol Ping command for the PC host name. You should also test the network interface configuration by Pinging another TCP/IP device that is connected to the network.

2. Install the RouteFinder software on the local PC. When installed click **Start | Programs | RouteFinder | Configuration Port Setup**, or double-click on the **Configuration Port Setup** icon in the **RouteFinder** program group.

3. The RouteFinder **Port Setup** dialog box is displayed.



   Verify that the **Communication Type** field is set to **IP.**

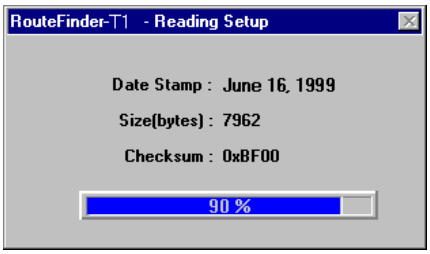
   In the **Router IP Address** field, enter the IP Address of the remote RouteFinder.

   Click **OK** when you are satisfied with your selections.

4. The Windows **Program Manager** menu is displayed.

   Double click the **RouteFinder Configuration** icon.

5. The **Reading Setup** dialog box is displayed.



6. The **Router Setup** dialog box is then displayed. This is the dialog box for the remote RouteFinder. You can select any of the available buttons and change the configuration (or setup) and download the changes to the remote RouteFinder. Refer to Chapter 4 for a description of the RouteFinder software. For definitions of each dialog box or fields within a dialog box, refer to the on-line **Help** provided in the software.

7. After you have changed the configuration of the remote RouteFinder, click the **Download Setup** button to update the configuration. The remote RouteFinder will be brought down, the new configuration written to the unit, and the unit will reboot.

8. Click the **Exit** button when the downloading is complete.

9. Click the **Router Configuration** icon in the Program Manager screen to verify that the RouteFinder is running.

Remote Management

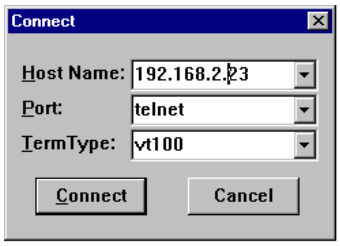
This section describes typical client applications that can be used to configure the RouteFinder remotely. It is important to note that although any subsequent changes to configuration can be made using these applications, the initial setup and configuration of the RouteFinder must be done on the local PC using the RouteFinder software provided with your unit.

Although establishing access to the RouteFinder varies between applications, the configuration functions mirror those of the RouteFinder software. For more information on RouteFinder software, refer to Chapter 4 - RouteFinder Software.

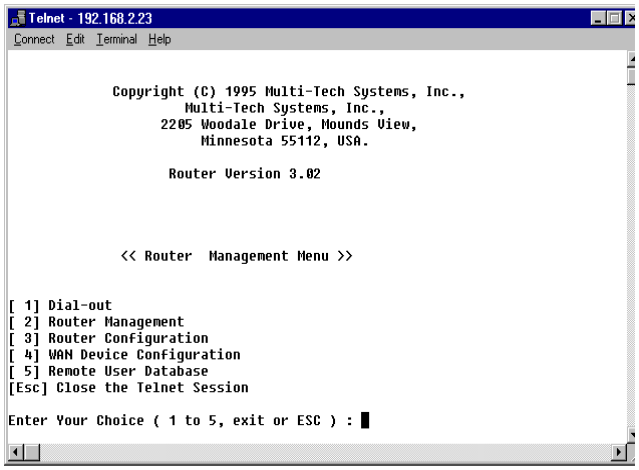
Telnet

A typical Telnet client application is described in this section. The RouteFinder has a built-in Telnet Server that enables Telnet client PCs to access the RouteFinder. A typical Telnet client is allowed to configure the RouteFinder and WAN device.

The TCP/IP stack has to be loaded before the Telnet client, a Windows application, can run. Double-Click the Telnet icon and a blank Telnet screen is displayed. Click the **Connect** menu; if the desired IP Address is listed in the drop-down menu, select it. Otherwise, select **Remote System** and when the **Connect** dialog box opens, enter the desired IP Address in the **Host Name** field and Click the **Connect** button.

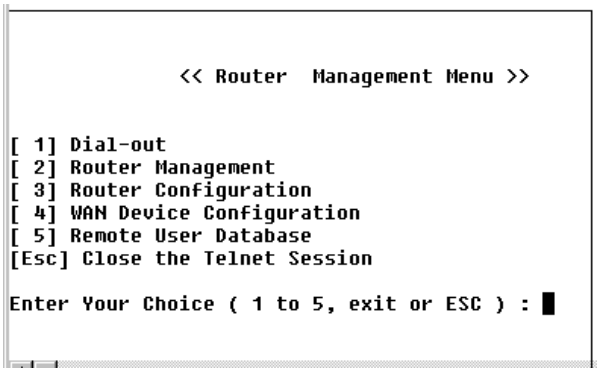


When you enter a valid Host Name (IP Address) and click the **Connect** button, you are immediately connected to the target RouteFinder and the Router Management Menu screen is displayed.



Router Management

The Router Management Menu provides five functional options in addition to the option of escaping and closing the Telnet session.



Dial-Out

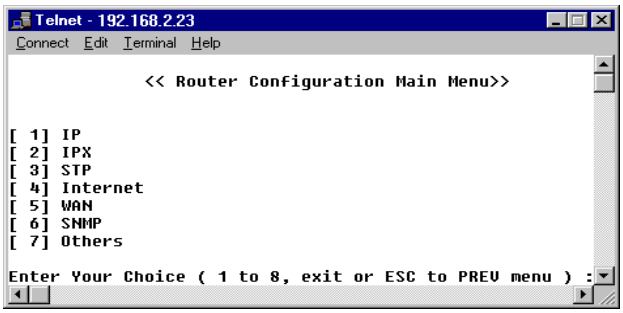
The Dial-out option (Option 1) on the Router Management Menu enables a Telnet user to configure the WAN port for a dial-out session. The default configuration of 115200 bps, 8N1 can be used for the dial-out session, or the user can specify each parameter for the port (e.g., the baud rate, the number of data bits, parity, or the number of stop bits). When the connection is established, anything entered on the keyboard is immediately presented to the WAN port. When the dial-out session is over, the WAN port reverts to its original configuration.

Router Management

The Router Management option (Option 2) enables a Telnet user to view router statistics, the User List, and system information. Another option enables the remote user to Reset the router.

Router Configuration

The Router Configuration option (Option 3) enables a Telnet user to view and change parameters on the protocol stacks, high or low level device drivers, enable or disable the supported servers, or view system information.



WAN Device Configuration

The WAN Device Configuration option (Option 4) allows a remote user (a Telnet client) to gain access to the WAN port (if available) on the RouteFinder.

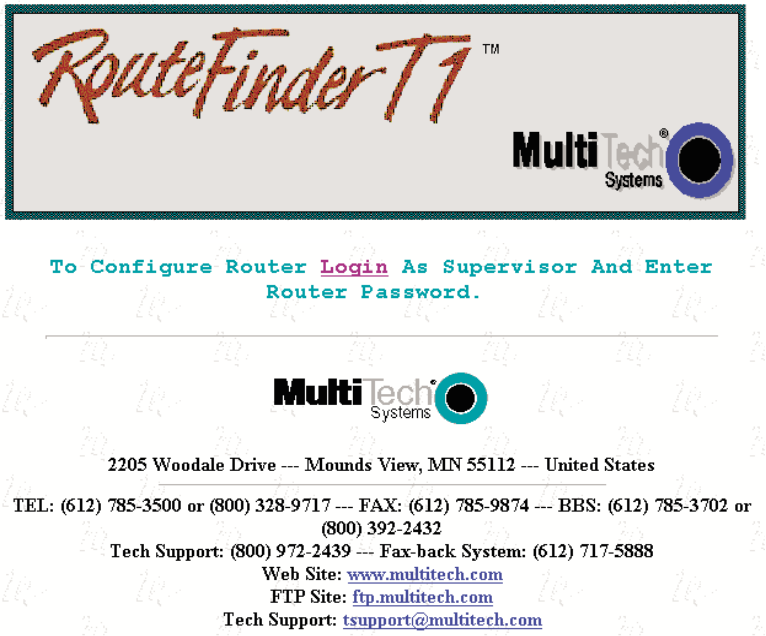
Remote User Database

The Remote User Database option (Option 5) allows a remote user to add user information such as Name and Password, callback information, and which protocol stacks to enable or disable.

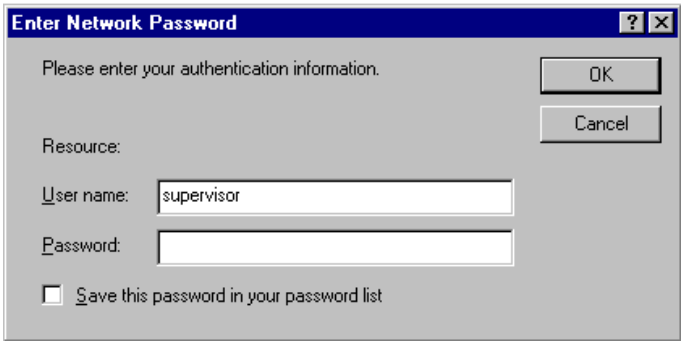
WEB Browser Management

The RouteFinder can be accessed from anywhere on the connected Internet through its built-in WEB Browser interface. To enable this function, you must check this option in Other setup. Depending on the rights of the user (read/write, or read only), it is possible to view the current parameters and statistics of the RouteFinder as well as configure and download setup changes to the unit.

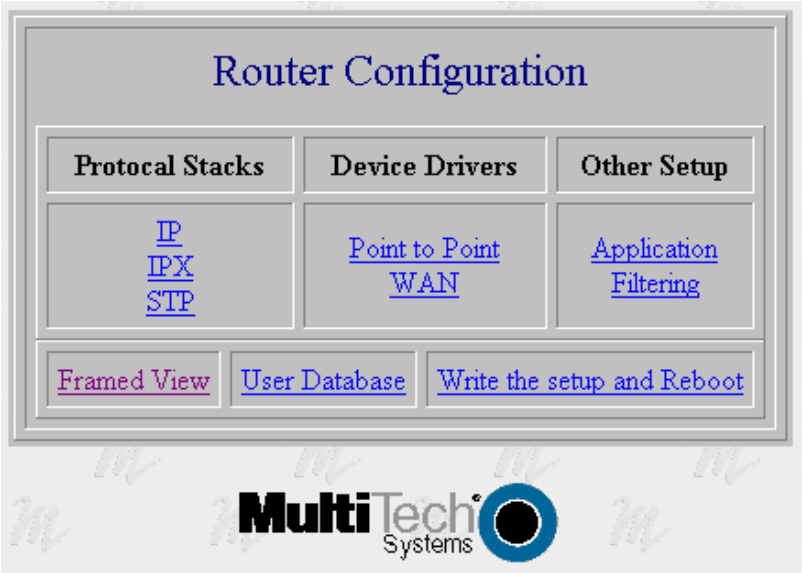
You can access RouteFinder configuration by typing the **IP Address** of the unit into the address line of your web browser. When the Welcome screen is displayed, click on the word **Login** to gain access to the RouteFinder.



The **Enter Network Password** screen is displayed.



Enter your **User name** and **Password**, then click on **OK** to go to the RouteFinder Configuration menu.



Note: The first user to access the RouteFinder will have *read/write* rights over the unit. All subsequent users will have *read only* rights, and therefore, some of the options within the WEB interface will be inactive (i.e., will not be linked).

RouteFinder™

Multi-Protocol Router with T1 DSU

Chapter 6 - Service, Warranty and Tech Support

MultiTech® Systems

Introduction

This chapter starts out with statements about your RouteFinder two-year warranty. The next section, Tech Support, should be read carefully if you have questions or problems with your RouteFinder. It includes the technical support phone numbers, space for recording your product information, and an explanation of how to send in your RouteFinder should you require service. The next section explains how to use our bulletin board service (BBS) and get support through the Internet.

Limited Warranty

Multi-Tech Systems, Inc. (“MTS”) warrants that its products will be free from defects in material or workmanship for a period of two years from the date of purchase, or if proof of purchase is not provided, two years from date of shipment. MTS MAKES NO OTHER WARRANTY, EXPRESSED OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by the customer or any party without MTS’s written authorization, or used in any manner inconsistent with MTS’s instructions.

MTS’s entire obligation under this warranty shall be limited (at MTS’s option) to repair or replacement of any products which prove to be defective within the warranty period, or, at MTS’s option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS’s factory transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PURCHASE PRICE FOR DEFECTIVE PRODUCTS.

On-line Warranty Registration

If you would like to register your RouteFinder electronically, you can do so at the following address:

http://www.multitech.com/register/

Tech Support

Multi-Tech Systems has an excellent staff of technical support personnel available to help you get the most out of your Multi-Tech product. If you have any questions about the operation of this unit, call 1-800-972-2439. Please fill out the RouteFinder information (below), and have it available when you call. If your RouteFinder requires service, the tech support specialist will guide you on how to send in your RouteFinder (refer to the next section).

Recording RouteFinder Information

Please fill in the following information on your Multi-Tech RouteFinder. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)

Model No.: _____
Serial No.: _____
Software Version: _____

The model and serial numbers are on the bottom of your RouteFinder.

Please note the status of your RouteFinder including LED indicators, screen messages, diagnostic test results, problems with a specific application, etc. Use the space below to note the RouteFinder status:

_____

_____

_____

_____

_____

_____

_____

_____

Service

If your tech support specialist decides that service is required, your RouteFinder may be sent (freight prepaid) to our factory. Return shipping charges will be paid by Multi-Tech Systems.

Include the following information with your RouteFinder:

- a description of the problem.
- return billing and return shipping addresses.
- contact name and phone number.
- check or purchase order number for payment if the RouteFinder is out of warranty. (Check with your technical support specialist for the standard repair charge for your RouteFinder).
- if possible, note the name of the technical support specialist with whom you spoke.

If you need to inquire about the status of the returned product, be prepared to provide the **serial number** of the product sent.

Send your RouteFinder to this address:

MULTI-TECH SYSTEMS, INC.

2205 WOODALE DRIVE

MOUNDS VIEW, MINNESOTA 55112

ATTN: SERVICE OR REPAIRS

You should also check with the supplier of your RouteFinder on the availability of loaner units and/or local service in your area.

The Multi-Tech BBS

For customers who do not have Internet access, Multi-Tech Systems maintains a bulletin board system (BBS) that mirrors its FTP site. Information available from the BBS includes new product information, product upgrade files, and problem-solving tips. The phone number for the Multi-Tech BBS is (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).

The BBS can be accessed by any asynchronous modem operating at 1200 bps to 56 Kbps at a setting of 8 bits, no parity, and 1 stop bit (8-N-1).

To log on to the Multi-Tech BBS

1. Set your communications program to **8-N-1**.
2. Dial our BBS at (800) 392-2432 (USA and Canada) or (612) 785-3702 (international and local).
3. At the prompts, type your first name, last name, and password; then press ENTER. If you are a first time caller, the BBS asks if your name is spelled correctly. If you answer yes, a questionnaire is displayed. You must complete the questionnaire to use the BBS on your first call.
4. Press ENTER until the Main Menu is displayed. From the Main Menu you have access to two areas: the Files Menu and News. For help on menu commands, type **?**.

To Download a file

If you know the file name

1. From the Main Menu, type **F** to access the Files Menu, then type **D**.
2. Enter the name of the file you wish to download from the BBS.
3. If a password is required, enter the password.
4. Answer **Y** or **N** to the automatic logoff question.
5. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).
6. If you select Zmodem, the transfer will begin automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most datacomm programs, the PAGE DOWN key initiates the download.)
7. When the download is complete, press ENTER to return to the File Menu.
8. To exit the BBS, type **G** and press ENTER.

If you don’t know the file name

1. From the Main Menu, type **F** to access the Files Menu. For a list of file areas, type **L**, press ENTER, then type **L** and press ENTER again. (If you do not type the second *L*, you will list all of the files on the BBS.)
2. Mark each file area you would like to examine by typing its list number and pressing ENTER.
3. Enter **L** to list all the files in the selected file areas. Enter **C** to go forward in the file list and **P** to go back.
4. To mark one or more files for download, type **M**, press ENTER, type the list numbers of the files, and press ENTER again.
5. Enter **D**. You will see a list of the files you have marked. Enter **E** if you would like to edit the list; otherwise enter **D** again to start the download process.
6. Select a file transfer protocol by typing the indicated letter, such as **Z** for Zmodem (the recommended protocol).

7. If you select Zmodem, the file will transfer automatically. If you select another protocol, you may have to initiate the transfer yourself. (In most data communications programs, the PAGE DOWN key initiates the download.)
8. When the download is complete, press ENTER to return to the File Menu.
9. To exit the BBS, type **G** and press ENTER.

About the Internet

If you prefer to receive technical support via the Internet, you can contact Tech Support via e-mail at the following address:

http:\\www.multitech.com

Multi-Tech's presence includes a Web site at:

http://www.multitech.com

and an ftp site at:

ftp://ftp.multitech.com

The ftp server mirrors the Multi-Tech BBS.

About Ordering Accessories

SupplyNet, Inc. can supply you with replacement transformers, cables and connectors for select Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989

Phone: 800 826-0279

Fax: 914 267-2420

Email: info@thesupplynet.com

Internet: http://www.thesupplynet.com

SupplyNet Online Ordering Instructions

1. Browse to http://www.thesupplynet.com. In the **Browse by Manufacturer** drop-down list, select **Multi-Tech** and click GO!
2. To order, type in quantity, and click Add to Order
3. Click Review Order to change your order
4. After you have selected all items, click Checkout to finalize the order. SupplyNet uses Verisign's Secure Socket Layer (SSL) technology to ensure your complete shopping security.

RouteFinder™

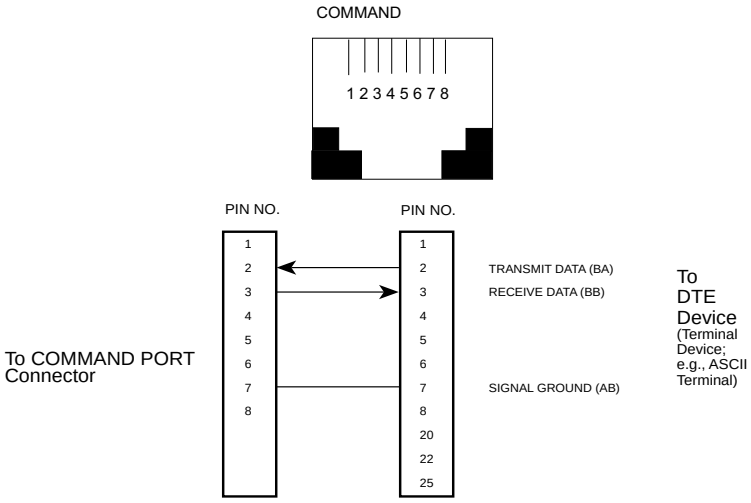
Multi-Protocol Router with T1 DSU

Appendixes

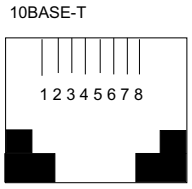
MultiTech® Systems

Appendix A - Cabling Diagrams

Command Port Cable



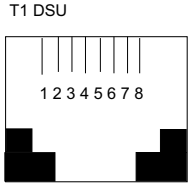
LAN Cable



10BASE-T (RJ-45)

Pin	Circuit	Signal Name
1	TD+	Data Transmit Positive
2	TD-	Data Transmit Negative
3	RD+	Data Receive Positive
6	RD-	Data Receive Negative

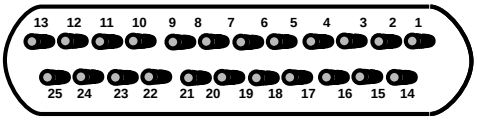
T1 DSU Cable



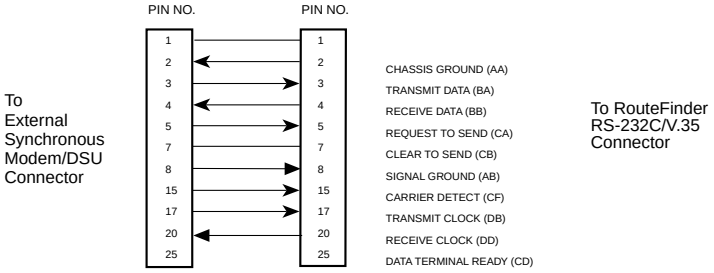
T1 DSU (RJ-48)

Pin	Signal Name
1	Receive Ring
2	Receive Tip
4	Transmit Ring
5	Transmit Tip

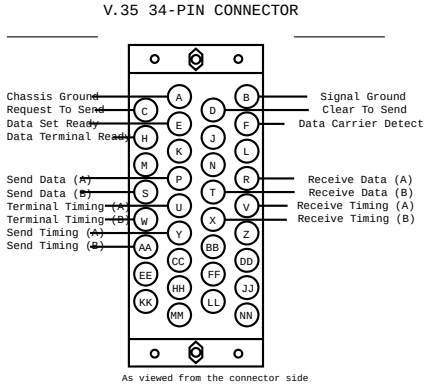
WAN 2 Cable (Dial back-up)

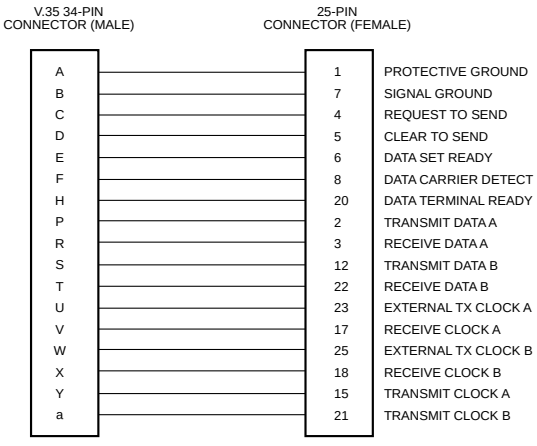


RS232C/V.24 * Link Cable



V.35 Adapter Cable Configured on an RS-232C/V.35**





* The RouteFinder RS-232C interface circuits have been designed to meet the electrical specificaitons given in EIA (Electronic Industries Association) RS-232C and CCITT (Consultative Committee International Telegraph and Telephone) V.24 Standards.

** When configured for V.35 interface operation, the V.35 adapter cable should be used. This cable uses a 25-pin female connector at one end and a 34-pin winchester male connector at the other end.

Appendix B - Script Language

The script file can be used to automate certain operations. The script file is a text file containing a sequence of commands. The structure of a script file is succinctly expressed by the following grammar.

Script Language Grammar

<program> =<declarations> <proc_declarations>
<declarations> ={<var_type> <identifier> {, <identifier> } ; }
<var_type> =INTEGER I STRING
<statement_list> ={<statement>}
<statement> =<elementary_statement> I <if_statement> I<for_statement> I
<while_statement> I <switch_statement>
<if_statement> =IF <expression> THEN <statement_list> {ELSE<statement_list> } ENDIF
<for_statement> =FOR <identifier>=<expression> TO IDOWNTO <expression} STEP
<expression> / DO <statement_list> ENDFOR
<while_statement> =WHILE <expression> DO <statement_list> ENDWHILE
<switch_statement> =SWITCH <expression> {CASE <integer_const> <statement_list> I
CASE <string_const> <statement_list> I
DEFAULT <statement_list> }
ENDSWITCH
<elementary_statement> =<identifier> = <expression> ; I <identifier> / (<expression>
{,<expression> }) /; I GOTO <identifier> ; I <identifier> : I ;
<expression> =<expression> OPERATOR <expression> I {<expression> } I /<expression>I
- <expression> I<identifier> / (<expression> {, <expression> }) /
OPERATOR = **<** I **<=** I > I >= I == I **!**= I **&&** I II I **+** I - I * I / I **!**
<proc_declaration> =PROC <identifier>/(<parameter_list>)} { :<vartype> };FORWARD ;
<proc_declaration> =PROC <identifier>/(<parameter_list>)} / : <vartype> / ;
<declarations> <statement_list>ENDPROC
<parameter_list> =<argument_list> { ; <argument_list>}
<argument_list>={VAR} <var_type> <identifier> {<identifier>}

Execution starts at the PROC main. PROC main cannot have any arguments. All the variables have to be declared before use. All procedures must be declared before calling. Recursion is allowed in procedures.

To define mutually recursive procedures, use the FORWARD directive to indicate that the procedure body is defined later in the source file. Procedures defined with the FORWARD directive should have all the parameters and return value (if any) specified, the actual definition of the procedure body should not contain the formal parameter list or the return value. An example of forward defined procedures is given below:

```
proc a(integer x,y) : integer,forward:
proc b(integer u,v) : integer,forward:
proc a;
        integer t;
        /*Some more code here. */

        t=b(x,y);
        /*Some more code here. */
        return(t);
endproc

proc b;
        return(a(u,v);
endproc
```

Argument to procedures can be passed by value or address. To pass an argument by address, prefix

the argument name in the formal parameter list by the keyword VAR; otherwise, the argument is passed by value. Only variables can be passed by address. Expressions like A+B, where A and B are integer variables can be passed by value but cannot be passed by address.

Two basic types of variables are supported:

INTEGER and STRING

In the STRING, since the ASCII null character is internally used to indicate the end of the sequence, it cannot be part of the string. All other characters, including extended ASCII characters can be part of the string.

There are two types of conditional constructs:

IF and SWITCH

The IF statement is a two-way branching construct. The condition can be an arbitrary expression. The condition in the IF statement should evaluate to an integer or real. If the expression in the IF statement evaluates to non-zero, the control enters the THEN statement, otherwise control enters the ELSE statement.

The SWITCH statement is a multi-way branching construct. The type of conditional expression should be either INTEGER or STRING. The value of the conditional expression is matched against the constraints given in the CASE options, if the value matches a CASE option value, control enters that CASE option. If the values do not match any of the CASE options, and if a DEFAULT option is provided, control continues at the DEFAULT option; otherwise control continues at the statement after the ENDSWITCH. If control enters one of the CASE or DEFAULT statements, all the statements up to the next ENDCASE statement are executed. Each CASE or DEFAULT statement should be terminated by a matching ENDCASE keyword. The SWITCH statement should be terminated by a ENDSWITCH keywork. The DEFAULT statement can be placed anywhere within the scope of the SWITCH statement. There can be only one DEFAULT statement.

There are two types of iterative constructs:

FOR and WHILE

The FOR construct sets the loop control variable to an initial value. The control variable is checked for bounds, and if within bounds, the <statement_list> given is executed; otherwise the loop execution terminates. After each execution of <statement_list>, the control variable is incremented or decremented by a certain value. This is computed as follows: if the STEP expression is given it is the value of the expression, else it is 1. The control variable is incremented if TO is specified, and is decremented if DOWNTO is specified. After updating the control variable the bounds check is done again. The keyword ENDFOR is mandatory at the end of the loop.

The WHILE loop has an expression and a <statement_list>. The expression is evaluated and if the expression is non-zero the <statement_list> is executed; otherwise the loop execution terminates. The keyword ENDWHILE is mandatory at the end of the loop.

Operator Precedence:

Operators are listed in the order of precedence

Unary Operators :-!(unary minus, logical negation)
Binary Operators :*/ **+ _< > <= >= == ! = &&** II

All the operators are left associative. Expressions are evaluated completely; so care must be taken while writing expressions. For example, expressions like (a !=0 && b / a) would create run time error.

Example Script:

```
proc main;
        string login_prompt;
        string user_name;
        string password_prompt;
        string password;
        string shell_menu;
        string shell_menu_response;
        integer timeout;

        timeout=10;
        login_prompt=”login:”;
        user_name=”user1”;
        password_prompt=”Password:”;
        password=”user1”;
        shell_menu=”choice:”;
        shell_menu_response=”1”;

        transmit(“A”);
        wait(1)
        transmit(“T^M”);
        waitfor (“OK”,10);

        transmit (“A”);
        wait (1);
        transmit (“T”);
        wait (1);
        transmit (“DT963^M”);

        if (waitfor (login_prompt,60))  then
                transmit (user_name);
                transmit (“^M”);
                if (waitfor (password_prompt,timeout))  then
                        transmit (password);
                        transmit (“^M”);
                        if (waitfor (shell_menu,timeout))  then
                        transmit (shell_menu_response);
                        transmit (“^M”);
        else
                        transmit (“Shell Menu Not Received^M”);
        endif
else
        transmit (“Password Prompt Not Received^M”);
        endif
else
        transmit (“Login Prompt Not Received^M”);
endif

Endproc
```

Appendix C - Changing Shunt Position

The RS-232/V.35 connector (WAN port) shunt must be moved to the V.35 position whenever you want to connect the RouteFinder to an external device with a V.35 interface. Do the following.

1. Ensure that all external cabling, including the power supply, is disconnected from the RouteFinder.
2. Turn the RouteFinder upside down and remove the cabinet mounting screw at the center back of the cabinet.

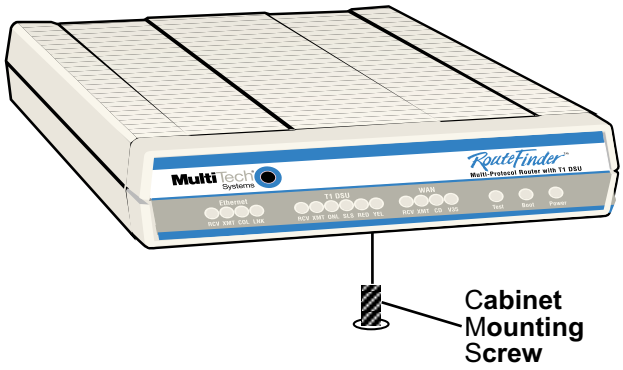


Figure C-1. Cabinet Mounting Screw

3. Turn the RouteFinder right side up, then slide the base out the rear of the cabinet.

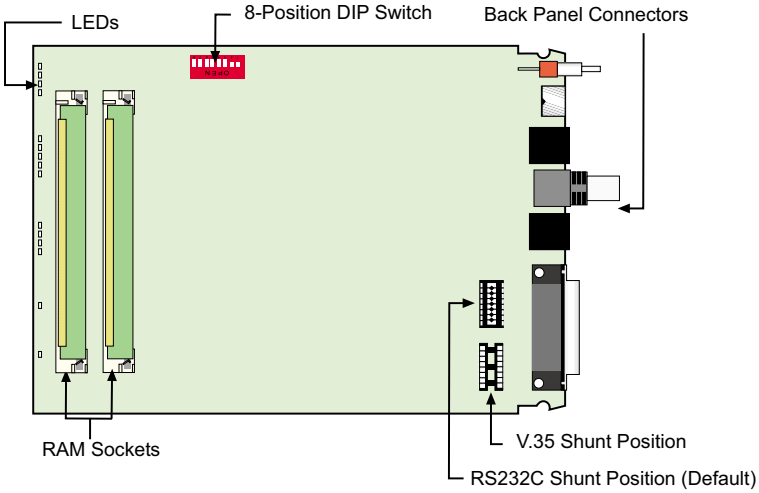


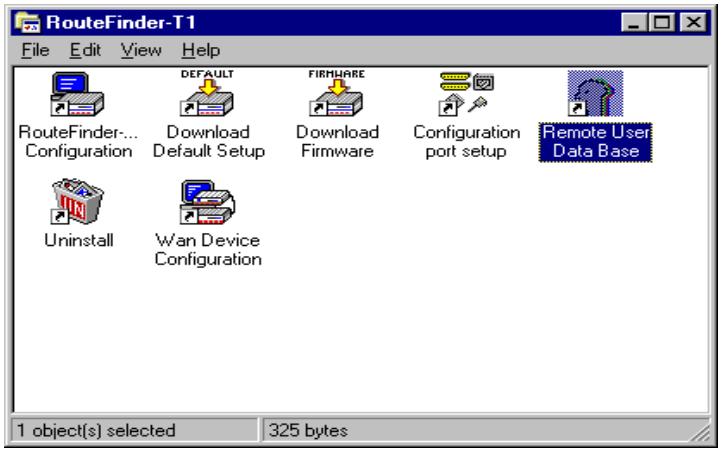
Figure C-2. Shunt Positions

4. Pry the shunt out of the default RS-232 position, then insert the shunt in the V.35 position for the RS-232/V.35 connector (WAN port). Refer to Figure C-2.
5. Slide the base all the way into the cabinet until it stops.
6. Turn the RouteFinder upside down and replace the cabinet mounting screw that was removed in step 2 (See Figure C-1).
7. Turn the RouteFinder right side up and connect the cables (Refer to the “Cabling your RouteFinder” section in Chapter 2).

Appendix D - Setting Up Your Remote User Database

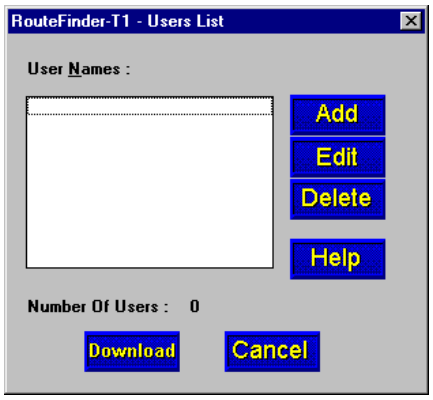
The Remote User Database option allows you to add and configure a list of users who need to access the RouteFinder remotely. Remote User Database supports remote dial-in users for user name, password, and port availability through the Command port. Each dial-in user needs an entry in this database. You can add remote users, remove users, or edit information in the database.

1. **Win3.1 users** - From the Program Manager, click the **Remote User Data Base** icon.



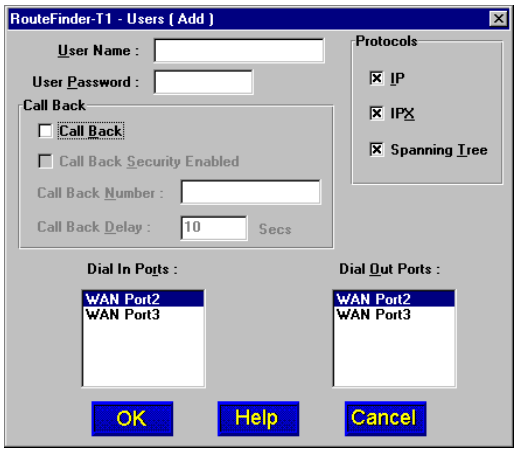
Win98/95/NT users - From your desktop, click the **Start** button, point to **Programs**, then **RouteFinder**, and then click **Remote User Data Base**.

2. The **Users List** dialog box is displayed.



Click the **Add User** button and

3. The **Add Users** dialog box is displayed.



4. Build your user database by filling in the following fields for each user.

   User Name.

   The User Name can have as many as 39 characters. All printable characters are permitted with the restriction that no blanks are allowed in the user name. In dial-in and dial-out applications, the user name is treated as a case insensitive string.

   User Password.

   The User Password can have as many as 7 characters. In places where the password is used as a character string, it is treated as a case insensitive string. Elsewhere (PPPs CHAP), it is treated as a case sensitive pattern.

   Call Back

   You have to click this check box in order to access the following three Call Back functions.

   - **Call Back Security Enabled**

     This parameter is of use in dial-in applications where the user is required to be called back at a specific location. Enabling this parameter (Alt-S) results in having the administrator assigning the call back parameters. Leave this function disabled if the user is to be allowed to choose the call back number and the call back delay.

   - **Call Back Number**

     The callback number is editable only if callback security is enabled (checked). This is the number where the user will be called back. The user **cannot** choose the location where he wants to be called back.

   - **Call Back Delay**

     Call back delay is editable only if callback security is enabled. This specifies the duration (in seconds) after which the user will be called back at the administrator-assigned number.

   Protocols

   This lets you select the protocol(s) the user is allowed to dial into the RouteFinder.

   Dial In Port

   WAN Port 2 is available for dialing into the RouteFinder.

   Dial Out Port

   WAN Port 2 is available for dialing out from the RouteFinder.

5. After each user is defined on the Add Users screen, click **OK** to display the updated Users List dialog box. Click **Add User** to continue adding users to your database.
6. When you have added all users to the data base, click **Download** to write the database to the RouteFinder.

Appendix E - TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol suite and related applications developed for the U.S. Department of Defense in the 1970s/80s specifically to permit different types of computers to communicate and exchange information with one another. TCP/IP is currently mandated as an official U.S. Department of Defense protocol and is also widely used in the UNIX community.

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. First, choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes educational organizations, .gov denotes government organizations). Next, determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You'll need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses.

Early IP implementations ran on hosts commonly interconnected by Ethernet local area networks (LAN). Every transmission on the LAN contains the local network, or medium access control (MAC), address of the source and destination nodes. The MAC address is 48-bits in length and is non-hierarchical; MAC addresses are never the same as IP addresses.

When a host needs to send a datagram to another host on the same network, the sending application must know both the IP and MAC addresses of the intended receiver. Unfortunately, the IP process may not know the MAC address of the receiver. The Address Resolution Protocol (ARP), described in RFC 826 (located at ftp://ds.internic.net/rfc/rfc826.txt) provides a mechanism for a host to determine a receiver's MAC address from the IP address. In the process, the host sends an ARP packet in a frame containing the MAC broadcast address; and then the ARP request advertises the destination IP address and asks for the associated MAC address. The station on the LAN that recognizes its own IP address will send an ARP response with its own MAC address. An ARP message is carried directly in an IP datagram.

Other address resolution procedures have also been defined, including those which allow a diskless processor to determine its IP address from its MAC address (Reverse ARP, or RARP), provides a mapping between an IP address and a frame relay virtual circuit identifier (Inverse ARP, or InARP), and provides a mapping between an IP address and ATM virtual path/channel identifiers (ATMARP).

The TCP/IP protocol suite comprises two protocols that correspond roughly to the OSI Transport and Session Layers; these protocols are called the Transmission Control Protocol and the User Datagram Protocol (UDP). Individual applications are referred to by a port identifier in TCP/UDP messages. The port identifier and IP address together form a "socket". Well-known port numbers on the server side of a connection include 20 (FTP data transfer), 21 (FTP control), 23 (Telnet), 25 (SMTP), 43 (whois), 70 (Gopher), 79 (finger), and 80 (HTTP).

TCP, described in RFC 793 (ftp://ds.internic.net/rfc/rfc793.txt) provides a virtual circuit (connection-oriented) communication service across the network. TCP includes rules for formatting messages, establishing and terminating virtual circuits, sequencing, flow control, and error correction. Most of the applications in the TCP/IP suite operate over the "reliable" transport service provided by TCP.

UDP, described in RFC 768 (ftp://ds.internic.net/rfc/rfc768.txt) provides an end-to-end datagram (connectionless) service. Some applications, such as those that involve a simple query and response, are better suited to the datagram service of UDP because there is no time lost to virtual circuit establishment and termination. UDP's primary function is to add a port number to the IP address to provide a socket for the application.

The Application Layer protocols are examples of common TCP/IP applications and utilities, which include:

- Telnet (Telecommunication Network): a virtual terminal protocol allowing a user logged on to one TCP/IP host to access other hosts on the network, described in RFC 854 (ftp://ds.internic.net/rfc/rfc854.txt).
- FTP: the File Transfer Protocol allows a user to transfer files between local and remote host computers per IETF RFC 959 (ftp://ds.internic.net/rfc/rfc959.txt).
- Archie: a utility that allows a user to search all registered anonymous FTP sites for files on a specified topic.
- Gopher: a tool that allows users to search through data repositories using a menu-driven, hierarchical interface, with links to other sites, per RFC 1436 (ftp://ds.internic.net/rfc/rfc1436.txt).
- SMTP: the Simple Mail Transfer Protocol is the standard protocol for the exchange of electronic mail over the Internet, per IETF RFC 821 (ftp://ds.internic.net/rfc/rfc821.txt).
- HTTP: the Hypertext Transfer Protocol is the basis for exchange of information over the World Wide Web (WWW). Various versions of HTTP are in use over the Internet, with HTTP version 1.0 (per RFC 1945) (ftp://ds.internic.net/rfc/rfc1945.txt) being the most current.
- HTML: WWW pages are written in the Hypertext Markup Language (HTML), an ASCII-based, platform-independent formatting language, per IETF RFC 1866 (ftp://ds.internic.net/rfc/rfc1866.txt).
- Finger: used to determine the status of other hosts and/or users, per IETF RFC 1288 (ftp://ds.internic.net/rfc/rfc1288.txt).
- POP: the Post Office Protocol defines a simple interface between a user's mail reader software and an electronic mail server; the current version is POP3, described in IETF RFC 1460 (ftp://ds.internic.net/rfc/rfc1460.txt).
- DNS: the Domain Name System defines the structure of Internet names and their association with IP addresses, as well as the association of mail, name, and other servers with domains.
- SNMP: the Simple Network Management Protocol defines procedures and management information databases for managing TCP/IP-based network devices. SNMP, defined by RFC 1157 (ftp://ds.internic.net/rfc/rfc1157.txt) is widely deployed in local and wide area network. SNMP Version 2 (SNMPv2), per RFC 1441< ftp://ds.internic.net/rfc/rfc1441.txt) adds security mechanisms that are missing in SNMP, but is also more complex.
- Ping: a utility that allows a user at one system to determine the status of other hosts and the latency in getting a message to that host. Ping uses ICMP Echo messages.
- Whois/NICNAME: Utilities that search databases for information about Internet domain and domain contact information, per RFC 954 (ftp://ds.internic.net/rfc/rfc954.txt).
- Traceroute: a tool that displays the route that packets will take when traveling to a remote host.

Internet Protocol (IP)

IP is the Internet standard protocol that tracks Internetwork node addresses, routes outgoing messages and recognizes incoming messages, allowing a message to cross multiple networks on the way to its final destination. The IPv6 Control Protocol (IPV6CP) is responsible for configuring, enabling, and disabling the IPv6 protocol modules on both ends of the point-to-point link. IPV6CP uses the same packet exchange mechanism as the Link Control Protocol (LCP). IPV6CP packets are not exchanged until PPP has reached the Network-Layer Protocol phase. IPV6CP packets received before this phase is reached are silently discarded. (See also TCP/IP.)

Before you install TCP/IP on your network, you need to establish your Internet addressing strategy. You first choose a domain name for your company. A domain name is the unique Internet name, usually the name of your business, that identifies your company. For example, Multi-Tech's domain name is multitech.com (where .com indicates this is a commercial organization; .edu denotes

educational organizations, .gov denotes government organizations, etc.). Next, you determine how many IP addresses you'll need. This depends on how many individual network segments you have, and how many systems on each segment need to be connected to the Internet. You need an IP address for each network interface on each computer and hardware device.

IP addresses are 32 bits long and come in two types: network and host. Network addresses come in five classes: A, B, C, D, and E. Each class of network address is allocated a certain number of host addresses. For example, a class B network can have a maximum of 65,534 hosts, while a class C network can have only 254. The class A and B addresses have been exhausted, and the class D and E addresses are reserved for special use. Consequently, companies now seeking an Internet connection are limited to class C addresses. The current demand for Internet connections will exhaust the current stock of 32-bit IP addresses. In response, Internet architects have proposed the next generation of IP addresses, IPng (IP Next Generation). It will feature 16-byte (128-bit) addressing, surpassing the capacities of 32-bit IP. Still in its design phase, IPng (also known as IPv6) is not expected to be widely deployed before the end of this century.

An IP address can serve only a single physical network. Therefore, if your organization has multiple physical networks, you must make them appear as one to external users. This is done via "subnetting", a complex procedure best left to ISPs and others experienced in IP addressing. Since IP addresses and domain names have no inherent connection, they are mapped together in databases stored on Domain Name Servers (DNS). If you decide to let an Internet Service Provider (ISP) administer your DNS server, the ISP can assist you with the domain name and IP address assignment necessary to configure your company's site-specific system information. Domain names and IP addresses are granted by the InterNIC. To check the availability of a specific name or to obtain more information, call the InterNIC at (703)742-4777.

Appendix F - Regulatory Information

Class A Statement

FCC Part 15

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

This device complies with Part 15 of the FCC rules.

Operation is subject to the following two conditions:

(1) This device may not cause harmful interference.

(2) This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

FCC Part 68 Telecom

1. This equipment complies with part 68 of the Federal Communications Commission Rules. On the outside surface of this equipment is a label that contains, among other information, the FCC registration number. This information must be provided to the telephone company.
2. As indicated below, the suitable jack (Universal Service Order Code connecting arrangement) for this equipment is shown. If applicable, the facility interface codes (FIC) and service order codes (SOC) are shown.
3. A FCC-compliant telephone cord and modular plug is provided with this equipment. This equipment is designed to be connected to the telephone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.
4. If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
5. The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications in order to maintain uninterrupted service.
6. If trouble is experienced with this equipment (the model of which is indicated below) please contact MultiTech Systems, Inc. at the address shown below for details of how to have repairs made. If the equipment is causing harm to the network, the telephone company may request you to remove the equipment from the network until the problem is resolved.
7. No repairs are to be made by you. Repairs are to be made only by MultiTech Systems or its licensees. Unauthorized repairs void registration and warranty.
8.

Manufacturer:	MultiTech Systems, Inc.
Trade Name:	RouteFinder
Model Number:	MTASR2-203
FCC Registration Number:	AU7USA-25529-DE-N
Modular Jack (USOC):	RJ48C
SOC Codes:	6.0N
Service Center in USA:	MultiTech Systems, Inc. 2205 Woodale Drive Mounds View, MN 55112 (612) 785-3500 Fax (612) 785-9874

Canadian Limitations Notice:

RINGER EQUIVALENCE NUMBER

NOTICE: The ringer equivalence number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface, The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence numbers of all the devices does not exceed 5.

NOTICE: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

CE

EMC and Safety Directive Compliance

The CE mark is affixed to this Multi-Tech product to confirm compliance with the following European Community Directives:

Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility;

and

Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;

each amended by

Council Directive 93/68/EEC of 22 July 1993 on the harmonization of CE marking requirements.

RouteFinder™

Multi-Protocol Router with T1 DSU

Glossary of Terms

MultiTech® Systems

A

Access: The T1 line element made up of two pairs of wire that the phone company brings to the customer premises. The Access portion ends with a connection at the local telco (LEC or RBOC).

Accunet Spectrum of Digital Services (ASDS): The AT&T 56K bps leased (private) line service. Similar to services of MCI and Sprint. ASDS is available in nx56/64K bps, where n=1, 2, 4, 6, 8, 12.

ACK (ACKnowledgement code) (pronounced "ack"): A communications code sent from a receiving modem to a transmitting modem to indicate that it is ready to accept data. It is also used to acknowledge the error-free receipt of transmitted data. Contrast with NAK.

Adaptive Differential Pulse Code Modulation (ADPCM): In multimedia applications, a technique in which pulse code modulation samples are compressed before they are stored on a disk. ADPCM, an extension of the PCM format, is a standard encoding format for storing audio information in a digital format. It reduced storage requirements by storing differences between successive digital samples rather than full values.

Address: A numbered location inside a computer. It's how the computer accesses its resources, like a video card, serial ports, memory, etc.

Address Resolution Protocol (ARP): A low-level protocol within the TCP/IP suite that "maps" IP addresses to corresponding Ethernet addresses. In other words, ARP is used to obtain the physical address when only the logical address is known. An ARP request with the IP address is braodcast onto the network. The node on which the IP address resides responds with the hardware addresss in order that the packets can be transmitted.

AMI line coding: One of two common methods of T1 line coding (with B8ZS). AMI line coding places restrictions on user data (B8ZS does not).

Analog signal: A waveform which has amplitude, frequency and phase, and which takes on a range of values between its maximum and minimum points.

Analog Transmission: One of two types of telecommunications which uses an analog signal as a carrier of voice, data, video, etc. An analog signal becomes a carrier when it is modulated by altering its phase, amplitude and frequency to correspond with the source signal. Compare with digital transmission.

Application Program Interface (API): A software module created to allow dissimilar, or incompatible applications programs to transfer information over a communications link. APIs may be simple or complex; they are commonly required to link PC applications with mainframe programs.

ASCII (American Standard Code for Information Interchange) (pronounced "askey"): A binary code for data that is used in communications and in many computers and terminals. The code is used to represent numbers, letters, punctuation and control characters. The basic ASCII code is a 7-bit character set which defines 128 possible characters. The extended ASCII file provides 255 characters.

Asynchronous Transfer Mode (ATM): A very high-speed method of transmission that uses fixed-size cells of 53 bytes to transfer information over fiber; also known as cell relay.

AT Commands: A standard set of commands used to configure various modem parameters, establish connections and disconnect. The "AT" is used to get the "attention" of the modem before the actual command is issued.

Availability: The measure of the time during which a circuit is ready for use; the complement of circuit "outage" (100% minus % outage = % available).

B

B7ZS (Bipolar 7 Zero Suppression) line coding: One method of T1 line coding (see also "B8ZS" and "AMI"). B7ZS line coding does not place restrictions on user data (AMI does).

B8ZS (Bipolar 8 Zero Suppression) line coding: One of two common methods of T1 line coding (with AMI). B8ZS line coding does not place restrictions on user data (AMI does). A coding method used to produce 64K bps "clear" transmission. (See also "B7ZS" and "AMI" line coding)

Backbone: 1. A set of nodes and their interconnecting links providing the primary data path across a network. 2. In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges. A backbone may be configured as a bus or as a ring. 3. In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected. 4. A common distribution core that provides all electrical power, gases, chemicals, and other services to the sectors of an automated wafer processing system.

Background: An activity that takes place in the PC while you are running another application. In other words, the active user interface does not correspond to the 'background' task.

Bandwidth: The transmission capacity of a computer channel, communications line or bus. It is expressed in cycles per second (hertz), the bandwidth being the difference between the lowest and highest frequencies transmitted. The range of usable frequencies that a transmission medium will pass without unacceptable attenuation or distortion. Bandwidth is a factor in determining the amount of information and the speed at which a medium can transmit data or other information.

Backward Explicit Congestion Notification (BECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiated in the opposite direction of the received frame. See also FECN (Forward Explicit Congestion Notification).

Basic Rate Interface (BRI): An ISDN access interface type comprised of two B-channels each at 64K bps and one D-channel at 64K bps (2B+D).

Bell Operating Companies (BOC): The family of corporations created during the divestiture of AT&T. BOCs are independent companies which service a specific region of the US. Also called Regional Bell Operating Companies (RBOCs).

Bell Pub 41450: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Bell Pub 62310: The Bell publication defining requirements for data format conversion, line conditioning, and termination for direct DDS connection.

Binary Synchronous Communication (BSC): A form of telecommunication line control that uses a standard set of transmission control characters and control character sequences, for binary synchronous transmission of binary-coded data between stations.

BiPolar Violation (BPV): The presence of two consecutive “one” bits of the same polarity on the T carrier line.

Bit (Binary digIT): A bit is the basis of the binary number system. It can take the value of 1 or 0. Bits are generally recognized as the electrical charge generated or stored by a computer that represent some portion of usable information.

Bit Error Rate Test (BERT): A device or routine that measures the quality of data transmission. A known bit pattern is transmitted, and the errors received are counted and a BER (bit error rate) is calculated. The BER is the ratio of received bits in error relative to the total number of bits received, expressed in a power of 10.

Bit robbing: The use of the least significant bit per channel in every sixth frame for signaling. The line signal bits “robbed” from the speech part conveys sufficient pre-ISDN telephony signaling information with the remaining line signal bits providing sufficient line signaling bits for recreating the original sound. See “robbed bit signaling”.

Blue Alarm: An error indication signal consisting of all 1s indicating disconnection or attached device failure. Contrast “Red Alarm” and “Yellow Alarm”.

Bps (bits per second): A unit to measure the speed at which data bits can be transmitted or received. Bps differs from baud when more than one bit is represented by a single cycle of the carrier.

Bridges: 1. A functional unit that interconnects two local area networks that use the same logical link protocol but may use different medium access control protocols. 2. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address. 3. In the connection of local loops, channels, or rings, the equipment and techniques used to match circuits and to facilitate accurate data transmission.

Buffer: A temporary storage register or Random Access Memory (RAM) used in all aspects of data communications which prevents data from being lost due to differences in transmission speed. Keyboards, serial ports, muxes and printers are a few examples of the devices that contain buffers.

Bus: A common channel between hardware devices either internally between components in a computer, or externally between stations in a communications network.

Byte: The unit of information a computer can handle at one time. The most common understanding is that a byte consists of 8 binary digits (bits), because that’s what computers can handle. A byte holds the equivalent of a single character (such as the letter A).

C

Call Setup Time: The time to establish a circuit-switched call between two points. Includes dialing, wait time, and CO/long distance service movement time.

Carrier Group Alarm (CGA): A T1 service alarm generated by a channel bank when an OOF condition occurs for a predefined length of time (usually 300mS to 2.5 seconds). The CGA causes the calls using a trunk to be dropped and for trunk conditioning to be applied.

Carrier signal: An analog signal with known frequency, amplitude and phase characteristics used as a transport facility for useful information. By knowing the original characteristics, a receiver can interpret any changes as modulations, and thereby recover the information.

CCITT (Consultative Committee for International Telephone and Telegraph): An advisory committee created and controlled by the United Nations and headquartered in Geneva whose purpose is to develop and to publish recommendations for worldwide standardization of telecommunications devices. CCITT has developed modem standards that are adapted primarily by PTT (post, telephone and telegraph) organizations that operate phone networks of countries outside of the U.S. See also ITU.

Central Office (CO): The lowest, or most basic level of switching in the PSTN (public switched telephone network). A business PABX or any residential phone connects to the PSTN at a central office.

Centrex: A multi-line service offered by operating telcos which provides, from the telco CO, functions and features comparable to those of a PBX for large business users. See also “Private Branch Exchange”, “Exchange”.

Channel: A data communications path between two computer devices. Can refer to a physical medium (e.g., UTP or coax), or to a specific carrier frequency.

Channel Bank: A device that acts as a converter, taking the digital signal from the T1 line into a phone system and converting it to the analog signals used by the phone system. A channel bank acts as a multiplexer, placing many slow-speed voice or data transactions on a single high-speed link.

Circuit-switched Network: A technology used by the PSTN that allocates a pair of conductors for the exclusive use of one communication path. Circuit switching allows multiple conversations on one talk path only if the end-users multiplex the signals prior to transmission.

Circuit Switching: The temporary connection of two or more communications channels using a fixed, non-shareable path through the network. Users have full use of the circuit until the connection is terminated.

Clear Channel: A transmission path where the full bandwidth is used (i.e., no bandwidth needed for signaling, carrier framing or control bits). A 64K bps digital circuit usually has 8K bps used for signaling. ISDN has two 64K bps circuits, and a 16K bps packet service of which part is used for signaling on the 64K channels.

Client-Server: In TCP/IP, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

Cluster Controller: A device that can control the input/output operations of more than one device connected to it. A cluster controller may be controlled by a program stored and executed in the unit, or it may be entirely controlled by hardware.

Committed Burst Size: The maximum number of bits that the frame relay network agrees to transfer during any measurement interval.

Committed Information Rate (CIR): An agreement a customer makes to use a certain minimum data transmission rate (in bps). The CIR is part of the frame relay service monthly billing, along with actual usage, that users pay to their frame relay service provider.

Compression: 1. The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. 2. In SNA, the replacement of a string of up to 64-repeated characters by an encoded control byte to reduce the length of the data stream to the LU-LU session partner. The encoded control byte is followed by the character that was repeated (unless that character is the prime compression character). 3. In Data Facility Hierarchical Storage Manager, the process of moving data instead of allocated space during migration and recall in order to release unused space. 4. Contrast with decompression.

COMx Port: A serial communications port on a PC.

congestion: A network condition where there is too much data traffic. The ITU I.233 standard defines congestion managemennt in terms of speed and burstiness.

congestion notification: The function in frame relay that ensures that user data transmitted at a rate higher than the CIR are allowed to slow down to the rate of the available network bandwidth.

Consecutive Severely Errored Seconds (CSES): An error condition that occurs when from 3 to 9 SES (Severely Errored Seconds) are logged consecutively.

Customer Premise Equipment (CPE): The generic term for data comm and/or terminal equipment that resides at the user site and is owned by the user with the following exclusions: Over voltage protection equipment, inside wiring, coin operated or pay telephones, “company-official” equipment, mobile telephone equipment, “911” equipment, equipment necessary for the provision of communications for national defense, or multiplexing equipment used to deliver multiple channels to the customer.

D

D4: the T1 4th generation channel bank.

D4 channelization: Refers to the compliance with AT&T TR 62411 for DS1 frame layout.

D4 framing: The T1 format for framing in AT&T D-Series channel banks, in which there are 12 separate 193-bit frames in a super-frame. A D4 framing bit is used to identify the channel and the signaling frame. Signalling for voice channels is carried in-band for every channel, along with the encoded voice. See “robbed-bit signaling”.

Data Communications Equipment (DCE): Any device which serves as the portal of entry from the user equipment to a telecommunications facility. A modem is a DCE for the telephone network (PSTN) that is commonly on site at the user’s premises. Packet Switched Networks have another level of DCE which is most often located at a central office.

Data Link Connection Identifier (DLCI): One of the six components of a frame relay frame. Its purpose is to distinguish separate virtual circuits across each access connection. Data coming into a frame relay node is thus allowed to be sent across the interface to the specified “address”. The DLCI is confirmed and relayed to its destination, or if the specification is in error, the frame is discarded.

Dataphone Digital Service (DDS): A private line digital service that offers 2400, 4800, 9600 and 56K bps data rates on an inter-LATA basis by AT&T and on an intra-LATA basis by the BOCs.

Data Service Unit (DSU): A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

Dedicated Line: A communication line that is not switched. The term leased line is more common.

Default: This is a preset value or option in software packages, or in hardware configuration, that is used unless you specify otherwise.

Device driver: Software that controls how a computer communicates with a device, such as a printer or mouse.

Digital Cross-connect System (DCS): The CO device which splits and redistributes the T1 bandwidth. the DCS takes time slots from various T1 lines and alters them to provide the needed connectivity. DCS connections are made with software at an administrator’s workstation.

Digital Data: Information represented by discrete values or conditions (contrast “Analog Data”).

Digital Loopback: A technique used for testing the circuitry of a communications device. Can be initiated locally, or remotely (via a telecommunications device). The tested device decodes and encodes a received test message, then echoes the message back. The results are compared with the original message to determine if corruption occurred en route.

Digital PBX: A Private Branch Exchange that operates internally on digital signals. See also “Exchange”.

Digital Service, level 0 (DS0): The world-wide standard speed (64K bps) for digital voice conversation using PCM (pulse coded modulation).

Digital Service, level 1 (DS1): The 1.544M bps voice standard (derived from an older Bell System standard) for digitized voice transmission in North America. The 1.544M bps consists of 24 digitally-encoded 64K bps voice channels (north America) and 2.048M bps (30 channels) elsewhere.

Digital Signal: A discrete or discontinuous signal (e.g., a sequence of voltage pulses). Digital devices, such as terminals and computers, transmit data as a series of electrical pulses which have discrete jumps rather than gradual changes.

Digital Signaling Rates (DSn): A hierarchical system for transmission rates, where “DS0” is 64K bps (equivalent to ISDN B channel), and DS1 is 1.5 Mbps (equivalent to ISDN PRI).

Digital Transmission: A method of electronic information transmission common between computers and other digital devices. Analog signals are waveforms: a combination of many possible voltages. A computer’s digital signal may be only “high” or “low” at any given time. Therefore, digital signals may be “cleaned up” (noise and distortion removed) and amplified during transmission.

Digitize: To convert an analog signal to a digital signal.

DIP switch (pronounced “dip switch”): A set of tiny toggle switches, built into a DIP (dual in-line package), used for setting configurable parameters on a PCB (printed circuit board).

Driver: A software module that interfaces between the Operating System and a specific hardware device (e.g., color monitors, printers, hard disks, etc.). Also known as a device driver.

Drop and Insert: The process where a portion of information carried in a transmission system is demodulated (“Dropped”) at an intermediate point and different information is included (“Inserted”) for subsequent transmission.

DTE (Data Terminal Equipment): A term used to include any device in a network which generates, stores or displays user information. DTE is a telecommunications term which usually refers to PCs, terminals, printers, etc.

DTMF (Dual-Tone MultiFrequency): A generic push-button concept made popular by AT&T TouchTone.

E

E&M: A telephony trunking system used for either switch-to-switch, or switch-to-network, or computer/telephone system-to-switch connection.

EIA: The Electronics Industries Association is a trade organization in Washington, DC that sets standards for use of its member companies. (See RS-232, RS-422, RS530.)

Encapsulation: A technique used by network-layer protocols in which a layer adds header information to the protocol data unit from the preceding layer. Also used in “enveloping” one protocol inside another for transmission. For example, IP inside IPX.

Errored Seconds (ES): Any second of operation that all 1.544M bits are not received exactly as transmitted. Contrast "Error Free Seconds".

Error Free Seconds (EFS): Any second of operation that all 1.544M bits are received exactly as transmitted. Contrast "Errored Seconds".

ESF Error Event: A T1 error condition that is logged when a CRC-6 error or an out-of-frame (OOF) error occurs.

Ethernet: A 10-megabit baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and transmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

Excess Zeros: A T1 error condition that is logged when more than 15 consecutive 0s or fewer than one 1 bit in 16 bits occurs.

Exchange: A unit (public or private) that can consist of one or more central offices established to serve a specified area. An exchange typically has a single rate of charges (tariffs) that has previously been approved by a regulatory group.

Exchange Area: A geographical area with a single uniform set of charges (tariffs), approved by a regulatory group, for telephone services. Calls between any two points within an exchange area are local calls. See also "Digital PBX", "PBX".

Exchange Termination (ET): The carrier's local exchange switch. Contrast with "Loop Termination - LT".

Explicit Congestion Management: The method used in frame relay to notify the terminal equipment that the network is overly busy. The use of FECN and BECN is called explicit congestion management. Some end-to-end protocols use FECN or BECN, but usually not both options together. With this method, a congestion condition is identified and fixed before it becomes critical. Contrast with "implicit congesion".

Extended Super Frame (ESF): One of two popular formats for framing bits on a T1 line. ESF framing has a 24-frame super-frame, where robbed bit signaling is inserted in the LSB (bit 8 of the DS-0 byte) of frames 6, 12, 18 and 24. ESF has more T1 error measurement capabilities than D4 framing. Both ESF and B8ZS are typically offered to provide clear channel service.

F

Failed Seconds: A test parameter where the circuit is unavailable for one full second.

Failed Signal: A T1 test parameter logged when there are more than 9 SES (Severely Errored Seconds).

Fax (facsimile): Refers to the bit-mapped rendition of a graphics-oriented document (fax) or to the electronic transmission of the image over telephone lines (faxing). Fax transmission differs from data transmission in that the former is a bit-mapped approximation of a graphical document and, therefore, cannot be accurately interpreted according to any character code.

Firmware: A category of memory chips that hold their content without electrical power, they include ROM, PROM, EPROM and EEPROM technologies. Firmware becomes "hard software" when holding program code.

Foreground: The application program currently running on and in control of the PC screen and keyboard. The area of the screen that occupies the active window. Compare with "background".

Fractional T1 (FT1): A digital data transmission rate between 56K bps (DS0 rate) and 1.544M bps (the full T1 rate - in North America). FT1 is typically provided on 4-wire (two copper pairs) UTP. Often used for video conferencing, imaging and LAN interconnection due to its low cost and relatively high speed. FT1 rates are offered in 64K bps multiples, usually up to 768K bps.

Frequency: A characteristic of an electrical or electronic signal which describes the periodic recurrence of cycles. Frequency is inversely proportional to the wavelength or pulse width of the signal (i.e., long wavelength signals have low frequencies and short wavelength signals yield high frequencies).

Foreign Exchange (FX): A CO trunk with access to a distant CO, allowing ease of access and flat-rate calls anywhere in the foreign exchange area.

Foreign Exchange Office (FXO): provides local telephone service from a CO outside of ("foreign" to) the subscriber's exchange area. In simple form, a user can pick up the phone in one city and receive a tone in the foreign city. Connecting a POTS telephone to a computer telephony system via a T1 link requires a channel bank configured for the FX connection. To generate a call from the POTS set to the computer telephony system, a FXO connection must be configured.

Foreign Exchange Station (FXS): See FX, FXO. To generate a call from the computer telephony system to the POTS set, an FXS connection must be configured.

Forward Explicit Congestion Notification (FECN): A bit that tells you that a certain frame on a particular logical connection has encountered heavy traffic. The bit provides notification that congestion-avoidance procedures should be initiatedin the same direction of the received frame. See also BECN (Backward Explicit Congestion Notification).

Frame: A group of data bits in a specific format to help network equipment recognize what the bits mean and how to process them. The bits are sent serially, with a flag at each end signifying the start and end of the frame.

Frame Relay: A form of packet switching that uses small packets and that requires less error checking than other forms of packet switching. Frame relay is effective for sending "bursty" data at high speeds (56/64K, 256K, and 1024K bps) over wide area networks. Frame Relay specifications are defined by ANSI documents ANSI T1.602, T1.606, T1S1/90-175, T1S1/90-213, and T1S1/90-214. In using frame relay, blocks of information (frames) are passed across a digital network interface using a "connection number" that is applied to each frame to distinguish between individual frames.

Frame Relay Forum: A non-profit organization of 300+ vendors and service providers, based in Foster City, CA, that are developing and deploying frame relay equipment.

Frame Relay Implementors Forum: A group of companies supporting a common specification for frame relay connection to link customer premises equipment to telco network equipment. Their specification supports ANSI frame relay specs and defines extensions such as local management.

Frame Relay Access Device (FRAD): A piece of equipment that acts as a concentrator or frame assembler/dissassember that can support multiple protocols and provide basic "routing" functions.

G

Gateway: 1. A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. 2. A network that connects hosts.

Graphical User Interface (GUI): A type of computer interface consisting of a visual metaphor of a real-world scene, often of a desktop. Within that scene are icons, representing actual objects, that the user can access and manipulate with a pointing device.

H

Handshaking: A process that two modems go through at the time of call setup to establish synchronization over the data communications link. It is a synchronization and negotiation process accomplished by the exchange of predefined, mutually recognized control codes.

Hexadecimal: A base 16 numbering system used to represent binary values. Hex uses the numbers 0-9 and the letters A-F: usually notated by an "h" (e.g., "4CF h", read "four charley fox, hex"). The result is that one hex digit represents a 4-bit value.

High-level Data Link Control (HDLC): An ISO standard, bit-oriented data communications protocol that provides nearly error-free data transfers.

I

Implicit congestion management: A method of informing the terminal that the network is busy. This method relies on the end-system protocol to detect and fix the congestion problem. (TCP/IP is an example of a protocol using only implicit congestion management.) See also "explicit congestion management".

In-band: Refers to the type of signalling over the conversion path on an ISDN call. Contrast "out-of-band".

Insufficient Ones: A T1 error condition that is logged when fewer than one 1 in 16 0s or less than 12.5 % average 1s density is received.

Internet Control Message Protocol (ICMP): As specified in RFC-792, ICMP provides a number of diagnostic functions and can send error packets to hosts. ICMP uses the basic support of IP and is an integral part of IP.

Inter Exchange Carrier (IEC): The long distance company (LE) who's central office provides the point of reference for T1 access. Any common carrier authorized by the FCC to carry customer transmissions between LATAs.

Internet: Refers to the computer network of many millions of university, government and private users around the world. Each user has a unique Internet Address.

Internet Address (IP Address): A unique 32-bit address for a specific TCP/IP host on a network. Normally printed in dotted decimal format (e.g., 129.128.44.227).

Internet Protocol (IP): A protocol used to route data from its source to its destination in an Internet enviroment. The Internet Protocol was designed to connect local area networks. Although there are many protocols that do this, IP refers to the global system of interconnecting computers. It is a highly distributed protocol (each machine only worries about sending data to the next step in the route).

Internetwork Packet Exchange (IPX): A NetWare communications protocol used to route messages from one node to another. IPX packets include network addresses and can be routed from one network to another. An IPX packet can occasionally get lost when crossing networks, thus IPX does not guarantee delivery of a complete message. Either the application has to provide that control, or NetWare's SPX protocol must be used.

Interoperable: Devices from different vendors that can exchange information using a standard's base protocol.

I/O Addresses: Locations within the I/O address space of your computer used by a device, such as an expansion card, a serial port, or an internal modem. The address is used for communication between software and a device.

IRQ Level (Interrupt Request Level): The notification a processor receives when another portion of the computer's hardware requires its attention. IRQs are numbered so that the device issuing the IRQ can be identified, and so IRQs can be prioritized.

ISA (Industry Standards Architecture) (pronounced "ice a"): The classic 8 or 16-bit architecture introduced with IBM's PC-AT computer.

ISDN (Integrated Services Digital Network): An International telecommunications standard for transmitting voice, video and data over a digital communications line. ISDN is a world-wide telecommunications service that uses digital transmission and switching technology to support voice and digital data communications. Frame relay was partially based on ISDN's data link layer protocol (LAPD). Frame relay can be used to transmit across ISDN services offering circuit-switched connection at 64K bps and higher speeds. Contrast Public Switched Telephone Network (PSTN).

ITU-TSS (formerly CCITT): International Telecommunications Union-Telecommunications Sector; the United Nations organization that prepares standards ("Recommendations") for resolving communications issues and problems.

J

No Entries.

K

Key Telephone System (KTS): Phone devices with multiple buttons that let you select incoming or outgoing CO phone lines directly. Similar in operation to a PBX, except with a KTS you don't have to dial a "9" to call outside the building.

Key Service Unit (KSU): A small device containing the switching electronics for a business key telephone system (KTS).

Key Set: A phone set with several buttons for call holding, line pickup, intercom, autodialing, etc. Also called a touchtone phone (Ericsson) and a KTS (Key Telephone Set).

L

LAPB: Link Access Procedure Balanced; based on the X.25 Layer 2 specification. A full-duplex, point-to-point, bit-synchronous protocol commonly used as a data link control protocol to interface X.25 DTEs. LAPB is the link initialization procedure that establishes and maintains communications between the DTE and the DCE.

LAPD: Link Access Protocol for the D-Channel; based on the ISDN Q.921 specification. A full-duplex point-to-point bit-synchronous link-level protocol for ISDN connections; different from LAPB in its framing sequence. Transmission is in units called "frames", and a frame may contain one or more X.25 packets.

Line Coding: The representation of 1s and 0s on a T1 line. The two methods of line coding commonly used, B8ZS and AMI, differ in the restrictions placed on user data. T1 line coding ensures that sufficient timing information is sent with the digital signal to ensure recovery of all the bits at the far end. Timing information on the T1 line is included in the form of 1s in the data stream; a long string of 0s in the data stream could cause problems recovering the data.

Line Termination (LT): The electronics at the ISDN network side of the user/network interface that complements the NT1 at the user side. The LT and the NT1 together provide the high-speed digital line signals required for BRI access.

Listed Directory Number (LDN): The main number assigned by the telco; the number listed in the phone directory and also provided by Directory Assistance. Some devices can have more than one LDN, such as ISDN devices that have one LDN for voice and another LDN for data.

Local Area Network (LAN): 1. A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. 2. A LAN does not use store-and-forward techniques. 3. A network in which a set of devices are connected to one another for a communication and that can be connected to a larger network.

Local Access and Transport Area (LATA): A post-divestiture geographical area generally equivalent to a Standard Metropolitan Statistical Area. At divestiture, the territory served by the Bell system was divided into approximately 161 LATAs. The Bell Operating Companies (BOCs) provide Intra-LATA services.

Local Exchange Carrier (LEC): The local phone company which provides local (i.e., not long distance) transmission services. AKA "telco". LECs provide T1 or FT1 access to LDCs (unless the T1 circuit is completely intra-LATA). Inter-LATA T1 circuits are made up of a combination of Access and Long Haul facilities.

Local Management Interface (LMI): A specification for frame relay equipment that defines status information exchange.

Local Loop: A transmission path, typically twisted-pair wire, between an individual subscriber and the nearest public telecommunications network switching center. The wires provide ISDN service, but require an NT1 at the user end and an LT at the network end. (AKA, “loop” or “subscriber loop”.)

Logical Link Control (LLC2): In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. The LLC2 protocol was developed by the IEEE 802 commitee and is common to all LAN standards.

Logical Unit (LU): A type of network accessible unit that enables end users to gain access to network resources and communicate with each other.

Long Haul: The T1 element that connects to the Access portion of the long distance company’s (LDC’s) central office. The LDC is commonly called the point of presence (POP). Each LDC has a number of POPs, located throughout the country. The LDC is also called an IEC (Inter Exchange Carrier).

Long Haul Communications: The type of phone call reaching outside of a local exchange (LE).

M

Management Information Base (MIB): A database of network management information used by the Common Management Information Protocol (CMIP) and the Simple Network Management Protocol (SNMP).

Megacom: An AT&T service with a normal WATS line (typically T1) between the customer premise and the AT&T serving class 4 CO are the customer’s responibility.

MegaLink: BellSouth’s leased T1 service.

Message: Associated with such terms as packet, frame, and segment. 1. In information theory, an ordered series of characters intended to convey information. 2. An assembly of characters and sometimes control codes that is transferred as an entry from an originator to one or more recipients.

Modem: A communications device that enables a computer to transmit information over a phone line. It converts the computer’s digital signals into analog signals to send over a phone line and converts them back to digital signals at the receiving end. Modems can be internal and fit into an expansion slot, or external and connect to a serial port.

Multiplexer (Mux): 1. A device that takes several input signals and combines them into a single output signal in such a manner that each of the input signals can be recovered. 2. A device capable of interleaving the events of two or more activities or capable of distributing the events of an interleaved sequence to the respective activities. 3. Putting multiple signals on a single channel.

Multiprotocol: A device that can interoperate with devices utilizing different network protocols.

RouteFinder: A secure gateway that provides multiple LAN users with high performance Internet access by functioning as a TCP/IP RouteFinder that resides on the outer edge of a firewall.

Multithreading: The ability of a software system to be able to handle more than one transaction concurrently. This is contrasted to the case where a single transaction is accepted and completely processed befor the next transaction processing is started.

N

Nailed Connection: A permanent or dedicated circuit of a previously switched circuit or circuits.

Nailed-up Circuit: A semi-permanent circuit established through a circuit-switching facility for point-to-point connectivity.

NAK (Negative Acknowledgment): Communications code used to indicate that a message was not properly received, or that a terminal does not wish to transmit. Contrast with ACK.

Network: A group of computers connected by cables or other means and using software that enables them to share equipment, such as printers and disk drives to exchange information.

Node: Any point within a network which has been assigned an address.

O

Object-Oriented: A method for structuring programs as hierarchically organized classes describing the data and operations of objects that may interact with other objects.

Office Channel Unit - Data Port (OCU-DP): The CO channel bank used as the interface between the customer’s DSU and the channel bank.

Off-hook: The condition of a device which has accessed a phone line (with or without using the line). In modem use, this is equivalent to a phone handset being picked up. Dialing and transmission are allowed, but incoming calls are not answered. Contrast “on-hook”.

Off Premise Extension (OPX): An extension or phone that terminates in a location other than that of the PBX. Commonly used to provide a corporate member with an extension of the PBX at home.

Ones Density: the measure of the number of logical 1s on a T1 line compared to a given total number of bits on that line; used for timing information in data recovery in AMI and B8ZS.

On-Hook: The condition of a device which has not accessed a phone line. In modem use, this is equivalent to a telephone handset that has not been picked up. In other words, it can receive an incoming call. Contrast “off-hook”.

Open Shortest Path First (OSPF): A hierarchical Interior Gateway Protocol (IGP) routing algorithm for IP that is a proposed standard for the Internet. OSPF incorporates least-cost routing, equal-cost routing, and load balancing.

Outage: The measure of the time during which a circuit is not available for use due to service interrupt. Outage is the complement of circuit “availability” (100% minus % available = % outage).

Out-of-band: Signaling that is separated from the channel carrying the information (e.g., the voice/data/video signal is separate from the carrier signal). Dialing and various other “supervisory” signals are included in the signaling element. Contrast “In-band” signaling.

Out of Frame (OOF): A T1 alarm condition that is logged on the loss of 2, 3 or 4 of 5 consecutive FT framing bits.

P

Packet: 1. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals and, possibly, error control information are arranged in a specific format. 2. Synonymous with data frame. 3. In TCP/IP, the unit of data passed across the interface between the Internet layer and the link layer. A packet includes an IP header and data. A packet can be a complete IP datagram or a fragment of an IP diagram. 4. In X.25, a data transmission information unit. A group of data and control characters, transferred as a unit, determined by the process of transmission. Commonly used data field lengths in packets are 128 or 256 bytes. 5. The field structure and format defined in the CCITT X.25 recommendation.

Packet Assembler/Dissembler (PAD): Used by devices to communicate over X.25 networks by building or stripping X.25 information on or from a packet.

Packet Data: The information format (“packetized”) used for packet-mode calls.

Packet Mode: Refers to the switching of chunks of information for different users using statistical multiplexing to send them over the same transmission facility.

Parity bit: An extra bit attached to each byte of synchronous data used to detect errors in transmission.

Permanent Virtual Circuit (PVC): A connection between two endpoints dedicated to a single user. In ISDN, PVCs are establised by network administration and are held for as long as the user subscribes to the service.

Physical Unit (PU): The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only.

Point of Presence (POP): The central office’s end points of the long distance carriers.

Point-to-Point Protocol (PPP): A protocol that lets a PC user access TCP/IP (Internet memeber) using an ISDN terminal adapter or a high-speed modem over a standard phone line.

Port: A location for input or output data exchange. Computers, muxes, etc. have ports for various purposes.

Primary Rate Interface (PRI): Used on ISDN. In North America, and Japan, PRI is one 64Kbps D channel and 23 B channels. Elsewhere, it is one D channel and 30 B channels.

Primitive: An abstract representation of interaction across the access points indicating that information is being passed between the service user and the service provider. The OSI Reference Model defines four types of primitives: Request, Indication, Response and Confirm.

Private Branch Exchange (PBX): A phone exchange located on the customer’s premises. The PBX provides a circuit switching facility for phone extension lines within the building, and access to the public phone network. See also “Exchange”.

PROM (Programmable Read Only Memory - pronounced “prom”): A permanent memory chip that can be programmed or filled by the customer after by the manufacturer has set initial values. Contrast with ROM.

Protocol: 1. A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. 2. In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. 3. In SNA, the meanings of and the sequencing rules for requests and responses used for managing the network, transferring data, and synchronizing the states of network components. 4. Synonymous with line control discipline.

PSTN (Public Switched Telephone Network): A worldwide public voice telephone network that is used as a telecommunications medium for the transmission of voice, data and other information.

Public Data Network (PDN): A packet-switched network that is available to the public for individual ("subscriber") use. Typically, controlled by a government or a national monopoly.

Public Switched Telephone Network (PSTN): The group of circuit-switching voice carriers, which are commonly used as analog data communications services.

Pulse Code Modulation (PCM): 1. In data communication, variation of a digital signal to represent information; for example, by means of pulse amplitude modulation (PAM), pulse duration modulation (PDM), or pulse position modulation (PPM). 2. Transmissions of analog information in digital form through sampling and encoding the samples with a fixed number of bits.

Pulse dialing: One of two methods of dialing a telephone, usually associated with rotary-dial phones. Compare with "tone dialing".

Q

Quantizing: The process of analog-to-digital conversion by assigning a range, from the contiguous analog values, to a discrete number.

R

Random Access Memory (RAM): A computer's primary workspace. All data must be stored in RAM (even for a short while), before software can use the processor to manipulate the data. Before a PC can do anything useful it must move programs from disk to RAM. When you turn it off, all information in RAM is lost.

Rate Enforcement: The concept in frame relay where frames sent faster than the CIR are to be carried only if the bandwidth is available, otherwise they are to be discarded. (The frame relay network assumes that anything exceeding the CIR is of low priority.) Rate enforcement makes sure that the network will not get so congested that it isn't able to meet the agreed on CIR.

Recognized Private Operating Agency (RPOA): A corporation, private or government-controlled, that provides telecommunications services. RPOAs, such as AT&T, participate as non-voting members in the CCITT.

Red Alarm: A T1 error condition generated when a local failure (e.g., loss of synchronization) exists for 2.5 seconds, causing a Carrier Group Alarm (CGA). See also "Blue Alarm" and "Yellow Alarm".

Request for Comment (RFC): A set of papers in which Internet standards (published and proposed), along with generally-accepted ideas, proposals, research results, etc. are published.

Ring Down Box: A device that emulates a CO by generating POTS calls for testing and product demos.

Ring Down Circuit: A tie line connecting phones where picking up one phone automatically rings another phone. A feature used for emergencies to alert the person at the other phone of the incoming call.

RJ-11: An industry standard interface used for connecting a telephone to a modular wall outlet; comes in 4-and 6-wire packages.

RJ-45: An 8-wire modular connector for voice and data circuits.

Robbed Bit Signaling: The popular T1 signaling mechanism where the A and B bits are sent by each side of the T1 termination and are "buried" in the voice data of each voice channel in the T1 circuit. Since the bits are "robbed" infrequently, voice quality remains relatively uncompromised. See "bit robbing". The robbed-bit signaling technique is used in D4 channel banks to convey signaling information. The eighth (least significant) bit of each of the 24 8-bit time slots is "robbed" every sixth frame to convey voice-related signaling information such as on-hook, off-hook, etc, for each channel.

Router: A device that connects two networks using the same networking protocol. It operates at the Network Layer (Layer 3) of the OSI model for forwarding decisions.

Routing Information Protocol (RIP): A distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

RS-232C: An EIA standard for a serial interface between computers and peripheral devices (modem, mouse, etc.). It uses a 25-pin DB-25, or a 9-pin DB-9 connector. The RS-232 standard defines the purposes, electrical characteristics and timing of the signals for each of the 25 lines.

RS-422: The EIA standard for a balanced interface with no accompanying physical connector. RS-422 products can use screw terminals, DB9, various DB25, and DB37 connectors.

RS-530: The EIA standard for the mechanical/electrical interface between DCEs and DTEs transmitting synchronous or asynchronous serial binary data. RS-530 provides for high data rates with the same connector used for RS-232; however, it is incompatible with RS-232.

S

Serial Port: The connector on a PC used to attach serial devices (those that need to receive data one bit after another), such as a mouse, a printer or a modem. This consists of a 9- or 25-pin connector that sends data in sequence (bit by bit). Serial ports are referred to as “COMx” ports, where x is 1 to 4 (i.e., COM1 through COM4). A serial port contains a conversion chip called a “UART” which translates between internal parallel and external serial formats.

Service: The requirements offered by an RPOA to its customers to satisfy specific telecommunications needs.

Severely Errored Seconds (SES): Refers to a typical T1 error event where an error burst occurs (a short term, high bit-error rate that is self-clearing). Per the ITU-T (CCITT) G.821: any second in which the BER is less than 1x10 -3 .

Signaling: The process of establishing, maintaining, accounting for, and terminating a connection between two endpoints (e.g., the user premises and the telco CO). Central office signals to the user premises can include ringing, dial tone, speech signals, etc. Signals from the user’s telephone can include off-hook, dialing, speech to far-end party, and on-hook signals. In-band signaling techniques include pulse and tone dialing. With common channel signaling, information is carried out-of-band.

Simple Network Management Protocol (SNMP): TCP/IP protocol that allows network management.

Simultaneous Voice Data (SVD): A technology for letting a user send data via a modem, and use a handset to talk to another user at the same time over the same connection. The alternative, making a second call, can be expensive or even impossible. The uses for SVD are telecommuting, videoconferencing, distant learning, tech support, etc.

Stop Bit: One of the variables used for timing in asynchronous data transmission. Depending on the devices, each character may be trailed by 1, 1.5, or 2 stop bits.

Superframe (D4): A T1 transmission format that consists of 12 DS1 frames, or 2316 bits. A DS1 frame consists of 193 bit positions. A frame overhead bit is in the first position, and it is used for frame and signaling phase alignment only.

Subscriber Loop: See “Local loop”.

Switched 56: A circuit-switched (full duplex digital synchronous data transmission) service that lets you dial a number and transmit data to it at 56K bps. It is a relatively low cost service, widely used in North America for telecommuting, videoconferencing and high speed data transfers. Many phone companies are (or will be) phasing out Switched 56 in favor of ISDN service.

Switched Virtual Circuit (SVC): A data transmission type where the connection is maintained only until the call is cleared.

Switched Line: In communications, a physical channel established by dynamically connecting one or more discrete segments. This connection lasts for the duration of the call, after which each segment can be used as part of a different channel. Contrast with leased line.

Switched Network: A network in which a temporary connection is established from one point via one or more segments.

Synchronous Data Link Control (SDLC): A discipline conforming to subsets of the Advanced Data Communications Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex, or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop.

Synchronous Transmission: The transmission of data which involves sending a group of characters in a packet. This is a common method of transmission between computers on a network or between modems. One or more synchronous characters are transmitted to confirm clocking before each packet of data is transmitted. Compare to Asynchronous Transmission.

Systems Network Architecture (SNA): The description of the logical structure, formats, protocols, and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks.

T

Tariff: The rate/availability schedule for telephone and ISDN services from a regulated service provider.

TCP/IP: A set of communication protocols that support peer-to-peer connectivity functions for both local and wide area networks.

T Carrier: The generic name for a digitally multiplexed carrier system. In the North American digital hierarchy, a T is used to designate a DS (digital signal) level hierarchy. Examples: T1 (DS1) is a 1.544 M bps 24-channel designation. In Europe, T1 is called E1. The T Carrier system was originally designed for transmitting digitized voice signals, but has since been adapted for digital data applications.

T1: A digital transmission link capable of 1.544M bps. T1 uses two pairs of normal UTP, and can handle 24 voice conversations, each digitized at 64K bps. T1 is a standard for digital transmission in the U.S., Canada, Japan and Hong Kong. T1 is the access method for high-speed services such as ATM, frame relay, and SMDS. See also T Carrier, T1 line and FT1.

T1 Channel Tests: A set of diagnostics that vary by carrier, used to verify a T1 channel operation. Can include Tone, Noise Level, Impulse Noise Level, Echo Cancelers, Gain, and Crosstalk testing.

T1 Framing: To digitize and encode analog voice signals requires 8000 samples per second (twice the highest voice frequency of 4000 Hz). Encoding in an 8-bit word provides the basic T1 block of 64K bps for voice transmission. This "Level 0 Signal, as its called, is represented by "DS-0", or Digital Signal at Level 0. 24 of these voice channels are combined into a serial bit stream (using TDM), on a frame-by-frame basis. A frame is a sample of all 24 channels; so adding in a framing bit gives a block of 193 bits (24x8+1=193). Frames are transmitted at 8000 per second (the required sample rate), creating a 1.544M (8000x193=1.544M) transmission rate.

T1 Line: A digital communications facility that functions as a 24-channel pathway for data or voice transmission. A T1 line is composed of two separate elements: the Access element and the Long Haul element.

T1 Mux: A device used to carry many sources of data on a T1 line. The T1 mux assigns each data source to distinct DS0 time slots within the T1 signal. Wide bandwidth signals take more than one time slot. Normal voice traffic or 56/64K bps data channels take one time slot. The T1 mux may use an internal or external T1 DSU; a "channel bank" device typically uses an external T1 CSU.

Transmission Control Protocol / Internet Program (TCP/IP): A multi-layer set of protocols developed by the US Department of Defense to link dissimilar computers across dissimilar and unreliable LANs.

Terminal: The screen and keyboard device used in a mainframe environment for interactive data entry. Terminals have no "box", which is to say they have no file storage or processing capabilities.

Terminal Adapter (TA): An ISDN DTE device for connecting a non-ISDN terminal device to the ISDN network. Similar to a protocol converter or an interface converter, a TA connects a non-ISDN device between the R and S interfaces. Typically a PC card.

Tie line: A dedicated circuit linking two points without having to dial a phone number (i.e., the line may be accessed by lifting the telephone handset or by pushing a button).

Time-Division Multiplexing (TDM): Division of a transmission facility into two or more channels by allotting the common channel to several different information channels, one at a time.

Time Slot: One of 24 channels within a T1 line. Each channel has a 64K bps maximum bandwidth. "Time slot" implies the time division multiplexing organization of the T1 signal.

Toll Call: A call to a location outside of your local service area (i.e., a long distance call).

Tone dialing: One of two methods of dialing a telephone, usually associated with Touch-Tone® (push button) phones. Compare with pulse dialing.

Topology: Physical layout of network components (cables, stations, gateways, and hubs). Three basic interconnection topologies are star, ring, and bus networks.

Transmission Control Protocol (TCP): A communications protocol used in Internet and in any network that follows the US Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It assumes that the Internet protocol is the underlying protocol.

Transport Layer: Layer 4 of the Open Systems Interconnection (OSI) model; provides reliable, end-to-end delivery of data, and detects transmission sequential errors.

Transport Protocol Data Unit (TPDU): A transport header, which is added to every message, contains destination and source addressing information that allows the end-to-end routing of messages in multi-layer NAC networks of high complexity. They are automatically added to messages as they enter the network and can be stripped off before being passed to the host or another device that does not support TPDU's.

Trivial File Transfer Protocol (TFTP): A UNIX-based file protocol. TFTP is a simplification of the earlier Simple File transfer Protocol (SFTP).

Trunk: Transmission links that interconnect switching offices.

TSR (terminate and stay resident): A software program that remains active and in memory after its user interface is closed. Similar to a daemon in UNIX environments.

Tunneling: Encapsulation data in an IP packet for transport across the Internet.

Twisted pair wiring: A type of cabling with one or more pairs of insulated wires wrapped around each other. An inexpensive wiring method used for LAN and telephone applications, also called UTP wiring.

U

UART (Universal Asynchronous Receiver/Transmitter) (pronounced “you art”): A chip that transmits and receives data on the serial port. It converts bytes into serial bits for transmission, and vice versa, and generates and strips the start and stop bits appended to each character.

User Datagram Protocol (UDP): A TCP/IP protocol describing how messages reach application programs within a destination computer. This protocol is normally bundled with IP-layer software. UDP is a transport layer, connectionless mode protocol, providing a (potentially unreliable, unsequenced, and/or duplicated) datagram mode of communication for delivery of packets to a remote or local user.

UNIX: An operating system developed by Bell Laboratories that features multiprogramming in a muti-user environment.

Unshielded Twisted Pair (UTP): Telephone-type wiring. Tansmission media for 10Base-T.

V

V.25bis: An ITU-T standard for synchronous communications between a mainframe or host and a modem using HDLC or other character-oriented protocol.

V.54: The ITU-T standard for local and remote loopback tests in modems, DCEs and DTEs. The four basic tests are:

- local digital loopback (tests DTE send and receive circuits),
- local analog loopback (tests local modem operation),
- remote analog loopback (tests comm link to the remote modem), and
- remote digital loopback (tests remote modem operation).

Virtual Circuit: A logical connection. Used in packet switching wherin a logical connection is established between two devices at the start of transmission. All information packets follow the same route and arrive in sequence (but do not necessarily carry a complete address).

W

Wide Area Network (WAN): 1. A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. 2. A data communications network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. Contrast with local area network (LAN).

Wide Area Telecommunications Service (WATS): A low-cost toll service offered by most long distance and local phone companies. Incoming (800 call service, or IN-WATS) and outgoing WATS are subscribed to separately, but over the same line.

X

X.25: ITU-T’s definition of a three-level packet-switching protocol to be used between packet-mode DTEs and network DCEs. X.25 corresponds with layer 3 of the 7-layer OSI model.

Y

Yellow Alarm: An error indication sent by the T1 device when it has not gotten a receive signal, or cannot synchronize on the receive signal received. Contrast “Red Alarm” and “Blue Alarm”.

Z

Zero Byte Time Slot Interchange (ZBTSI): A method for allowing 64K bps unrestricted user data (allowing all 0s in the user data). An alternative to (but not as popular as) B8ZS.

Index

P

R

S

T

U

V

W